VOLUNTARY VOTING SYSTEM GUIDELINES

VOLUNTARY VOTING SYSTEM GUIDELINES

Volume II

National Certification Testing Guidelines

Voluntary Voting System Guidelines

Table of Contents

Volume I Voting System Performance Guidelines

Volume II National Certification Testing Guidelines

Voluntary Voting System Guidelines Overview

Table of Contents

Voluntary Voting System Guidelines Overview

The United States Congress passed the Help America Vote Act of 2002 (HAVA) to modernize the administration of federal elections, marking the first time in our nation's history that the federal government has funded an election reform effort. HAVA provides federal funding to help the states meet the law's uniform and non-discretionary administrative requirements, which include the following new programs and procedures: 1) provisional voting, 2) voting information, 3) statewide voter registration lists and identification requirements for first-time registrants, 4) administrative complaint procedures, and 5) updated and upgraded voting equipment.

HAVA also established the U.S. Election Assistance Commission (EAC) to administer the federal funding and to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. Section 202 directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software. The purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems.

This document, the *Voluntary Voting System Guidelines* (referred to herein as the *Guidelines* and/or *VVSG*), is the third iteration of national level voting system standards that has been developed. The Federal Election Commission published the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems* in 1990. This was followed by the *Voting Systems Standards* in 2002.

As required by HAVA, the EAC formed the Technical Guidelines Development Committee (TGDC) to develop an initial set of recommendations for the *Guidelines*. This committee of 15 experts began their work in July 2004 and submitted their recommendations to the EAC in the 9-month timeline prescribed by HAVA. The TGDC was provided with technical support by the National Institute for Standards and Technology (NIST), which was given nearly $3 million dollars by the EAC to complete this work.

The EAC reviewed and revised the TGDC recommendations and, as required by HAVA, published the proposed *Guidelines* for a 90 day public comment period. The document was also provided to both the Board of Advisors and the Standards Board for their review and comment. During the comment period the EAC conducted 3 public hearings on the *Guidelines* in New York City, Pasadena and Denver. Over 6000 comments were received from the public and the Boards. Each of these comments was reviewed and considered by the EAC in consultation with NIST in the development of this final version.

Purpose and Scope of the *Guidelines*

The purpose of the *Voluntary Voting System Guidelines* is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems. The *VVSG* specifies the functional requirements, performance characteristics, documentation requirements, and test evaluation criteria for the national certification of voting systems. The *VVSG* is composed of two volumes: Volume I, *Voting System Performance Guidelines* and Volume II, *National Certification Testing Guidelines.*

Effective Date

The 2005 *Voluntary Voting System Guidelines* will take effect 24 months after their final adoption in December 2005 by the EAC. At that time, all new systems submitted for national certification will be tested for conformance with these guidelines. In addition, if a modification to a system qualified or certified to a previous standard is submitted for national certification after this date, every component of the modified system will be tested against the 2005 *VVSG.* All previous versions of national standards will become obsolete at this time. This effective date provision does not have any impact on the mandatory January 1, 2006, deadline for states to comply with the HAVA Section 301 requirements.

Summary of Changes

Volume I of the *Guidelines*, entitled *Voting System Performance Guidelines,* includes new requirements for usability, accessibility, voting system software distribution, generation of software reference information, validation of software during voting system setup, and the use of wireless communications. System functional requirements have been revised to comply with HAVA Section 301 requirements. Environmental criteria have been updated. This volume also includes requirements for a voter verifiable paper audit trail component for direct-recording electronic voting systems for use by states that require this feature. In addition, this volume includes an updated glossary and a conformance clause.

Volume II of the *Guidelines*, entitled *National Certification Testing Guidelines*, has been revised to reflect the new EAC process for national certification of voting systems. This process was initiated in 2005 and replaces the voting system qualification process conducted by the National Association of State Election Directors (NASED) since 1994. In addition, revisions have been made to the testing procedures to reflect new requirements for the conduct of usability and accessibility testing. Volume II also includes an updated appendix on procedures for testing system error rates. Terminology in both volumes has been revised to reflect new terminology introduced by HAVA.

Volume I: *Voting System Performance Guidelines* Summary

Volume I, the *Voting System Performance Guidelines*, describes the requirements for the electronic components of voting systems. It is intended for use by the broadest audience, including voting system developers, manufacturers and suppliers; voting system testing labs; state organizations that certify systems prior to procurement; state and local election officials who procure and deploy voting systems; and public interest organizations that have an interest in voting systems and voting system standards. It contains the following sections:

Section I describes the purpose and scope of the *Voting System Performance Guidelines.*

Section 2 describes the functional capabilities required of voting systems. This section has been revised to reflect HAVA Section 301 requirements.

Section 3 describes new standards that make voting systems more usable and accessible for as many eligible citizens as possible, whatever their physical abilities, language skills, or experience with technology. This section reflects the HAVA 301 (a)(3) accessibility requirements.

Sections 4 through 6 describe specific performance standards for election system hardware, software, telecommunications, and security. Environmental criteria have been updated in Section 4.

Section 7 describes voting system security requirements and includes new requirements for voting system software distribution, generation of software reference information, validation of software during system setup, and the use of wireless. It also includes requirements for voter verifiable paper audit trail components for direct-recording electronic voting systems.

Sections 8 and 9 describe requirements for vendor quality assurance and configuration management practices and the documentation about these practices required for the EAC certification process.

Appendix A contains a glossary of terms.

Appendix B provides a list of related standards documents incorporated into the *Guidelines* by reference, documents used in the preparation of the *Guidelines*, and referenced legislation.

Appendix C presents an introductory discussion of independent verification systems as a potential concept for future voting system security design.

Appendix D contains technical guidance on color, contrast and text size adjustment for individuals with low vision or color blindness.

Volume II: *National Certification Testing Guidelines* Summary

Volume II, the *National Certification Testing Guidelines*, is a complementary document to Volume I. Volume II provides an overview and specific detail of the national certification testing process, which is performed by independent voting system test labs accredited by the EAC. It is intended principally for use by vendors: test labs: and election officials who certify, procure, and accept voting systems. This volume contains the following sections:

Section 1 describes the purpose of the *National Certification Testing Guidelines*.

Section 2 provides a description of the Technical Data Package that vendors are required to submit with their system for certification testing.

Section 3 describes the basic functionality testing requirements.

Sections 4 through 6 define the requirements for hardware, software and system integration testing. Section 6 has been revised to reflect new requirements for usability and accessibility testing.

Section 7 describes the required examination of vendor quality assurance and configuration management practices.

Appendix A provides the requirements for the National Certification Test Plan that is prepared by the voting system test lab and provided to the EAC for review.

Appendix B describes the scope and content of the National Certification Test Report which is prepared by the test lab and delivered to the EAC along with a recommendation for certification.

Appendix C describes the guiding principles used to design the voting system certification testing process. It also contains a revised section on testing system error rates.

National Certification Testing Guidelines

Table of Contents

1 Introduction

Table of Contents

1 Introduction

1.1 Overview of the National Certification Testing Guidelines

Volume II, *National Certification Testing Guidelines*, is a complementary document to Volume I, *Voting System Performance Guidelines.* Volume I specifies the requirements that a voting system must conform to in order to be nationally certified as acceptable for use in federal elections. Volume II describes the testing process that is designed to provide a documented independent verification by an accredited voting system test lab that a voting system has been demonstrated to conform to the Volume I requirements and therefore should receive national certification.

Volume II, *National Certification Testing Guidelines*, provides the specific detail about the testing process that is needed for the accredited test labs, voting system vendors and election officials participating in the system certification process.

Independent Accredited Test Labs: Test labs that are accredited to perform conformance testing of voting systems will use Volume II to guide the development of test plans, the testing of systems, and the preparation of test reports and recommendations for granting national certification. Organizations wishing to become accredited as voting system test labs can refer to Volume II to understand the requirements and obligations placed on an accredited voting system test lab.

Voting System Vendors: Voting system vendors will use Volume II to guide the design, construction, documentation, internal testing, and maintenance of voting systems. They will also use this document to help define the responsibilities of organizations that support the system, such as suppliers, testers and consultants.

Election Officials: Election officials will use Volume II to guide their state certification, procurement, and acceptance processes and requirements. Certification at the state level may entail system conformance with additional requirements beyond those required for national certification to comply with state election laws or procedures.

1.2 Overview of the National Certification Testing Process

Certification testing encompasses the examination and testing of software; tests of hardware under conditions simulating the intended storage, operation, transportation, and maintenance environments; the inspection and evaluation of system documentation; and operational tests to validate system performance and functioning under normal and abnormal conditions. The testing also evaluates the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with stated system design and performance specifications, and the vendor's documented quality

assurance and configuration management practices. The tests address individual system components or elements, as well as the integrated system as a whole.

Beginning in 1994, the National Association of State Election Directors (NASED) began accrediting Independent Test Authorities for the purpose of conducting qualification testing of voting systems. The qualification testing process was originally based on the 1990 voting system standards and evolved to encompass the new requirements contained in the 2002 version of the standards.

The Help America Vote Act (HAVA) directs the U.S. Election Assistance Commission (EAC) to provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories. HAVA also introduces different terminology for these functions. Under the EAC process, test labs are "accredited" and voting systems are "certified." The term "standards" has been replaced with the term "*Guidelines*." As prescribed by HAVA, the EAC process was initially based on the 2002 Voting Systems Standards and will transition to the revised standards issued through the 2005 *Voluntary Voting System Guidelines*.

1.3 Testing Scope

The national certification testing process is intended to discover vulnerabilities that, should they appear in actual election use, could result in failure to complete election operations in a satisfactory manner. There are four focuses that guide the overall process:

- Operational accuracy in the recording and processing of voting data, as measured by target error rate, for which the maximum acceptable error rate is no more than one in ten million ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions
- Operational failures or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots
- System performance and function under normal and abnormal conditions
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system

1.3.1 Test Categories

The certification test procedure is presented in several parts:

- Functionality testing
- Hardware testing
- Software evaluation

- System level integration tests, including audits
- Examination of documented vendor practices for quality assurance and for configuration management

In practice, there may be concurrent indications of hardware and software function, or failure to function, during certain examinations and tests. Operating tests of hardware partially exercise the software as well and therefore supplement software testing. Security tests exercise hardware, software and communications capabilities. Documentation review conducted during software qualification supplements the review undertaken for system-level testing.

Not all systems being tested are required to complete all categories of testing. For example, if a previously certified system has had hardware modifications, the system may be subject only to non-operating environmental stress testing of the modified component and system level integration testing. If a system consisting of general purpose COTS hardware, or one that was previously certified has had modifications to its software, the system is subject only to software testing and system level integration tests, not hardware testing. However, in all cases the system documentation and configuration management records will be examined to confirm that they completely and accurately reflect the components and component versions that comprise the voting system.

1.3.1.1 Focus of Functionality Tests

Functionality testing is performed to confirm the functional capabilities of a voting system. The accredited test lab designs and performs procedures to test a voting system against the requirements outlined in Volume I, Section 2. In order to best complement the diversity of the voting systems industry, this part of the testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate depending on the system's use of specific technologies and configurations, the system capabilities, and the outcomes of previous testing.

1.3.1.2 Focus of Hardware Tests

Hardware testing begins with non-operating tests that require the use of an environmental test facility. These are followed by operating tests that are performed partly in an environmental facility and partly in a standard accredited test laboratory or shop environment.
The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to the various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standards (MIL-STD) 810F, modified where appropriate, and include such tests as: bench handling, vibration, low and high temperature, and humidity.

The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This period of operation ensures with confidence that the hardware meets or exceeds the minimum requirements for reliability, data reading, and

processing accuracy contained in Volume I, Section 4. The procedure emphasizes equipment operability and data accuracy; it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions, in most cases, has been reduced from that specified in the Military Standards to reflect commercial and industrial practice.

1.3.1.3 Focus of Software Evaluation

The software tests encompass a number of interrelated examinations, involving assessment of application source code for its compliance with the requirements spelled out in Volume I, Section 5. Essentially, the accredited test lab will look at programming completeness, consistency, correctness, modifiability, structure, and traceability, along with its modularity and construction. The code inspection will be followed by a series of functional tests to verify the proper performance of all system functions controlled by the software.

The accredited test lab may inspect COTS generated software source code in the preparation of test plans and conduct some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.

1.3.1.4 Focus of System Integration Tests

The functionality, hardware, and software certification tests supplement a fuller evaluation performed by the system level integration tests. System level tests focus on these aspects jointly, throughout the full range of system operations. They include tests of fully integrated system components, internal and external system interfaces, usability and accessibility, and security. During this process election management functions, ballot-counting logic, and system capacity are exercised. The process also includes the Physical Configuration Audit (PCA) and the Functional Configuration Audit (FCA).

The accredited test lab tests the interface of all system modules and subsystems with each other against the vendor's specifications. Some systems use telecommunications capabilities as defined in Volume 1, Section 6. For those systems that do use such capabilities, components that are located at the poll site or separate vote counting site are tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the vendor (e.g., public telephone networks), the accredited test lab tests the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

The security tests focus on the ability of the system to detect, prevent, log, and recover from a broad range of security risks as identified in Volume 1, Section 7. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems are tested for effective access control and physical data security. For systems that use public telecommunications networks, to transmit election

management data or official election results (such as ballots or tabulated results), security tests are conducted to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. The tests determine if the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for qualification. The accredited test lab may meet these testing requirements by confirming the proper implementation of proven commercial security software.

The interface between the voting system and its users, both voters and election officials, is a key element of effective system operation and confidence in the system. Guidelines for usability by individual voters with disabilities have been defined in Volume 1, Section 3. Voting systems are tested to ensure that an accessible voting station is included in the system configuration and that its design and operation conforms to these guidelines.

The Physical Configuration Audit (PCA) compares the voting system components submitted for qualification to the vendor's technical documentation and confirms that the documentation submitted meets the requirements of the *Guidelines*. As part of the PCA, the accredited test lab also witnesses the build of the executable system to ensure that the qualified executable release is built from the tested components.

The Functional Configuration Audit (FCA) is an exhaustive verification of every system function and combination of functions cited in the vendor's documentation. Through use, the FCA verifies the accuracy and completeness of the system Technical Data Package (TDP). The various options of software counting logic that are claimed in the vendor's documentation shall be tested during the system-level FCA. Generic test ballots or test entry data for DRE systems, representing particular sequences of ballot-counting events, will test the counting logic during this audit.

1.3.1.5 Focus of Vendor Documentation Examination

The accredited test lab reviews the documentation submitted by the vendor for its completeness and accuracy in describing the system. The accredited test lab also reviews the documentation to evaluate the extent to which it conforms to the requirements outlined in Volume 1, Sections 8 and 9 for vendor configuration and quality assurance practices. The accredited test lab examines the conformance of other documentation and information provided by the vendor with the vendor's documented practices for quality assurance and configuration management.

The *Guidelines* do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the accredited test lab conducts several activities while at the vendor site to witness the system build that enable assessment of the vendor's quality assurance and configuration management practices and conformance with them. These include surveys, interviews with individuals at all levels of the development team, and examination of selected internal work products such as system change requests and problem tracking logs.

1.4 Testing Sequence

The overall testing process progresses through several stages involving pre-testing, testing, and post-testing activities. National certification testing involves a series of physical tests and other examinations that are conducted in a particular sequence. The sequence is intended to maximize overall testing effectiveness, as well as conduct testing in as efficient a manner as possible. The accredited test lab will follow the general sequence outlined below. Test anomalies and errors are communicated to the system vendor throughout the process.

a. Initial examination of the system and the technical documentation provided by the vendor to ensure that all components and documentation needed to conduct testing have been submitted, and to help determine the scope and level of effort of testing needed

b. Examination of the vendor's Quality Assurance Program and Configuration Management Plan

c. Development of a detailed system test plan that reflects the scope and complexity of the system, and the status of system certification (i.e., initial certification or a re-certification to incorporate modifications)

d. Code review for selected software components

e. Witnessing of a system 'build' conducted by the vendor to conclusively establish the system version and components being tested

f. Operational testing of hardware components, including environmental tests, to ensure that operational performance requirements are achieved

g. Functional and performance testing of hardware components

h. System installation testing and testing of related documentation for system installation and diagnostic testing

i. Functional and performance testing of software components

j. Functional and performance testing of the integrated system, including testing of the full scope of system functionality, performance tests for telecommunications and security; and examination and testing of the System Operations Manual

k. Examination of the system maintenance manual

l. Preparation of the National Certification Test Report

m. Delivery of the National Certification Test Report to the EAC

1.5 Documentation Submitted by Vendor

The vendor shall submit all the documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the accredited test lab for conducting system certification testing. This documentation collectively is referred to as the Technical Data Package (TDP). The TDP provides information that defines the voting system design, method of operation, and related resources. It provides a system overview and documents the system's functionality, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures, and personnel deployment and training requirements. It also documents the vendor's configuration management plan and quality assurance program. If another version of the system was previously certified, the TDP would also include appropriate system change notes.

1.6 Voting Equipment Submitted by Vendor

Vendors may seek to market a complete voting system or an interoperable component of a voting system. In all instances, vendors shall submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed plus the other components with which the vendor recommends that the component be used. The system submitted for testing shall meet the following requirements:

a. The hardware submitted for certification testing shall be equivalent, in form and function, to the actual production version of the hardware units or the COTS hardware specified for use in the TDP

b. The software submitted for certification testing shall be the exact software that will be used in production units

c. Engineering or developmental prototypes are not acceptable, unless the vendor can show that the equipment to be tested is equivalent to standard production units both in performance and construction

d. Benchmark directory listings shall be submitted for all software/firmware elements (and associated documentation) included in the vendor's release as they would normally be installed upon setup and installation

1.7 Test Applicability

Certification tests are conducted for new systems seeking initial certification as well as for modified versions of systems that have been certified.

1.7.1 General Applicability

Voting system hardware, software, communications and documentation are examined and tested to determine suitability for elections use. Examination and testing addresses the broad range of system functionality and components, including system functionality for pre-voting, voting, and post-voting functions. All products custom designed for election use shall be tested in accordance with the applicable procedures contained in this section. COTS hardware, system software and communications components with proven performance in commercial applications other than elections, however, are exempted from certain portions of the test as long as such products are not modified for use in a voting system. Compatibility of these products with other components of the voting system shall be determined through functional tests integrating these products with the remainder of the system.

1.7.1.1 Hardware

Specifically, the hardware test requirements shall apply in full to all equipment used in a voting system with the exception of the following:

a. Commercially available models of general purpose information technology equipment that have been designed to an ANSI or IEEE standard, have a documented history of successful performance for relevant requirements of the standards, and have demonstrated compatibility with the voting system components with which they interface

b. Production models of special purpose information technology equipment that have a documented history of successful performance under conditions equivalent to election use for relevant requirements of the standards and that have demonstrated compatibility with the voting system components with which they interface

c. Any ancillary devices that do not perform ballot definition, election database maintenance, ballot reading, ballot data processing, or the production of an official output report; and that do not interact with these system functions (e.g. modems used to broadcast results to the press, printers used to generate unofficial reports, or CRTs used to monitor the vote counting process)

This equipment shall be subject to functional and operating tests performed during software evaluation and system level testing. However, it need not undergo hardware non-operating tests. If the system is composed entirely of off-the-shelf hardware, then the system also shall not be subject to the 48-hour environmental chamber segment of the hardware operating tests.

1.7.1.2 Software

Software certification is applicable to the following:

a. Application programs that control and carry out ballot processing, commencing with the definition of a ballot, and including processing of the ballot image (either from physical ballots or electronically activated images), and ending with the system's access to memory for the generation of output reports

b. Specialized compilers and specialized operating systems associated with ballot processing

c. Standard compilers and operating systems that have been modified for use in the vote counting process

Specialized software for ballot preparation, election programming, vote recording, vote tabulation, vote consolidation and reporting, and audit trail production shall be subjected to code inspection. Functional testing of all these programs during software evaluation and system-level testing shall exercise any specially tailored software off-line from the ballot counting process (e.g. software for preparing ballots and broadcasting results).

1.7.2 Modifications to Certified Systems

Changes introduced after the system has completed certified testing will necessitate further review.

1.7.2.1 General Requirements for Modifications

The accredited test lab will determine tests necessary to certify the modified system based on a review of the nature and scope of changes, and other submitted information including the system documentation, vendor test documentation, configuration management records, and quality assurance information. Based on this review, the accredited test lab may:

a. Determine that a review of all change documentation against the baseline materials is sufficient for recommendation for certification

b. Determine that all changes must be retested against the previously certified version. This will include review of changes to source code, review of all updates to the TDP, and performance of system level and functional tests

c. Determine that the scope of the changes is substantial and will require a complete retest of the hardware, software, and/or telecommunications

1.7.2.2 Basis for Limited Testing Determinations

The accredited test lab may determine that a modified system will be subject only to limited certification testing if the vendor demonstrates that the change does not affect demonstrated compliance with these *Guidelines* for:

a. Performance of voting system functions

b. Voting system security and privacy

c. Overall flow of system control

d. The manner in which ballots are defined and interpreted, or voting data are processed

Limited testing is intended to facilitate the correction of defects, the incorporation of improvements, the enhancement of portability and flexibility, and the integration of vote-counting software with other systems and election software.

1.8 Certification Test Process

The certification test process may be performed by one or more accredited test labs that together perform the full scope of tests required. Where multiple accredited test labs are involved, testing shall be conducted first for the voting system hardware, firmware, and related documentation; then for the system software and communications; and finally for the integrated system as a whole. Voting system hardware and firmware testing may be performed by one accredited test lab independently of the other testing performed by other accredited test labs. Testing may be coordinated across accredited test labs so that hardware/firmware tested by one accredited test lab can be used in the overall system tests performed by another accredited test lab.

When multiple accredited test labs are being used, the development of the National Certification Test Plan (see Appendix A) and the National Certification Test Report (see Appendix B) shall be coordinated by a lead accredited test lab. The lead lab is responsible for ensuring that all testing has been performed and documented in accordance with the *Guidelines*.

Whether one or more accredited test labs are used, the testing generally consists of three phases:

- Pre-test Activities
- National Certification Testing
- National Certification Report Issuance and Post-test Activities

1.8.1 Pre-test Activities

Pre-test activities include the request for initiation of testing and the pre-test preparation.

1.8.1.1 Initiation of Testing

Certification testing shall be conducted at the request of the vendor, consistent with the provision of the *Guidelines*. The vendor shall:

a. Request the performance of certification testing from among the accredited testing laboratories

b. Enter into formal agreement with the accredited test lab for the performance of testing

c. Prepare and submit materials required for testing consistent with the requirements of the *Guidelines*

Certification testing shall be conducted for the initial version of a voting system as well as for all subsequent changes to the system prior to release for sale or for installation. As described in Subsection 1.6.2, the nature and scope of testing for system changes or new versions shall be determined by the accredited test lab based on the nature and scope of the modifications to the system and on the quality of system documentation and configuration management records submitted by the vendor.

1.8.1.2 Pre-test Preparation

Pre-test preparation encompasses the following activities:

a. The vendor shall prepare and submit a complete TDP to the accredited test lab. The TDP should consist of the materials described in Section 2

b. The accredited test lab shall perform an initial review of the TDP for completeness and clarity and request additional information as required

c. The vendor shall provide additional information, if requested by the accredited test lab

d. The vendor and accredited test lab shall enter into an agreement for the testing to be performed by the accredited test lab in exchange for payment by the vendor

e. The vendor shall deliver to the accredited test lab all hardware and software needed to perform testing

1.8.2 Certification Testing

Certification testing encompasses the preparation of a test plan, the establishment of the appropriate test conditions, the use of appropriate test fixtures, the witness of the system build and installation, the maintenance of certification test data, and the evaluation of the data resulting from tests and examinations.

1.8.2.1 National Certification Test Plan

The accredited test lab shall prepare a National Certification Test Plan to define all tests and procedures required to demonstrate compliance with the *Guidelines*, including:

Verifying or checking equipment operational status by means of manufacturer operating procedures

a. Establishing the test environment or the special environment required to perform the test

b. Initiating and completing operating modes or conditions necessary to evaluate the specific performance characteristic under test

c. Measuring and recording the value or range of values for the characteristic to be tested, demonstrating expected performance levels

d. Verifying, as above, that the equipment is still in normal condition and status after all required measurements have been obtained

e. Confirming that documentation submitted by the vendor corresponds to the actual configuration and operation of the system

f. Confirming that documented vendor practices for quality assurance and configuration management comply with the *Guidelines*

A recommended outline for the test plan and the details of required testing are contained in Appendix A.

1.8.2.2 Certification Test Conditions

The accredited test lab may perform the tests in any facility capable of supporting the test environment. The following practices shall be employed:

a. Preparations for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one independent, qualified observer in the form of an accredited testing laboratory, which shall certify that all test and data acquisition requirements have been satisfied

b. When a test is to be performed at "standard" or "ambient" conditions, this requirement shall refer to a nominal laboratory or office environment, with a temperature in the range of 68 to 75 degrees Fahrenheit, and prevailing atmospheric pressure and relative humidity

c. Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

   i. Temperature +/- 4 degrees F

   ii. Electrical supply voltage +/- 2 voltage alternating current

1.8.2.3 Certification Test Fixtures

The accredited test lab may use test fixtures or ancillary devices to facilitate testing. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data:

a. For systems that use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems that rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable

b. The accredited test lab may use a simulation device, and appropriate software, to speed up the process of testing and eliminate human error in casting test ballots, provided that the simulation covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure shall be used to validate the proper operation of those portions of the system not tested by the simulator

c. If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself

1.8.2.4 Witness of System Build and Installation

Although most testing is conducted at facilities operated by the accredited test lab, a key element of voting system testing shall be conducted at either the vendor site or the accredited test lab site. The accredited test lab responsible for testing voting system software, telecommunications, and integrated system operation (i.e., system level testing) shall witness the final system build, encompassing hardware, software and communications, and the version of associated records and documentation. The system elements witnessed, including their specific versions, shall become the specific system version that is recommended for certification.

1.8.2.5 Certification Test Data Requirements

The following test data practices shall be employed:

a. A test log of the procedure shall be maintained. This log shall identify the system and equipment by model and serial number

b. Test environment conditions shall be noted

c. All operating steps, the identity and quantity of simulated ballots, annotations of output reports, the elapsed time for each procedure step, and observations of equipment performance and, in the case of non-operating hardware tests, the condition of the equipment shall be recorded

1.8.2.6 Certification Test Practices

The accredited test lab shall conduct the examinations and tests defined in the National Certification Test Plan such that all applicable tests identified in Volume II, *National Certification Testing Guidelines* are executed to determine compliance with the voting system requirements described in Volume I. The accredited testing laboratory shall evaluate data resulting from examinations and tests, employing the following practices:

a. If any malfunction or data error is detected that would be classified as a relevant failure using the criteria in Volume II, *National Certification Testing Guidelines*, its occurrence, and the duration of operating time preceding it, shall be recorded for inclusion in the analysis of data obtained from the test, and the test shall be interrupted

b. If a malfunction is due to a defect in software, then the test shall be terminated and system returned to the vendor for correction

c. If the malfunction is other than a software defect, and if corrective action is taken to restore the equipment to a fully operational condition within 8 hours, then the test may be resumed at the point of suspension

d. If the test is suspended for an extended period of time, the accredited test lab shall maintain a record of the procedures that have been satisfactorily completed. When testing is resumed at a later date, repetition of the successfully completed procedures may be waived, provided that no design or manufacturing change has been made that would invalidate the earlier test results

e. Any and all failures that occurred as a result of a deficiency shall be classified as purged, and test results shall be evaluated as though the failure or failures had not occurred, if the:

i. Vendor submits a design, manufacturing, or packaging change notice to correct the deficiency, together with test data to verify the adequacy of the change

ii. Examiner of the equipment agrees that the proposed change will correct the deficiency

iii. Vendor certifies that the change will be incorporated into all existing and future production units

f. If corrective action cannot be successfully taken as defined above, then the test shall be terminated, and the equipment shall be rejected

1.8.3 Post-test Activities

Certification report issuance and post-test activities encompass the activities described below.

a. The accredited test lab may issue interim reports to the vendor, informing the vendor of the testing status, findings to date, and other information.

b. The accredited test lab shall prepare a National Certification Test Report that confirms the voting system has passed the required testing. This report shall include the date testing was completed, the specific system version addressed by the report, the version numbers of all system elements separately identified with a version number by the vendor, and the scope of tests conducted. A recommended outline for the test report is contained in Appendix B.

c. Where a system is tested by multiple accredited test labs, the lead accredited test lab shall prepare a consolidated National Certification Test Report.

d. The accredited test lab shall deliver the report to the vendor and to the EAC.

e. Upon review and acceptance of the test report, EAC shall issue a Certification Number for the system to the vendor and to the accredited test lab. The issuance of a Certification Number indicates that the system has been tested by the accredited test lab for compliance with the *Guidelines.*

f. This number applies to the system as a whole only for the configuration and versions of the system elements tested and identified in the National Certification Test Report. The Certification Number does not apply to individual system components or untested configurations.

g. The EAC Certification Number is intended for use by the states and their jurisdictions to support state and jurisdiction processes concerning voting systems. States and their jurisdictions shall request National Certification Test Reports based on the EAC

Certification Number to support their voting system certification and procurement processes.

1.8.4 Resolution of Testing Issues

Prior to the transition of this function to the EAC, the NASED Voting Systems Board (the Board) was responsible for resolving questions about the application of the *Guidelines* in the testing of voting systems. The EAC will have a process for the accredited test labs, vendors and election officials to request an interpretation of the *Guidelines*. The interpretation will be publicly documented for reference by interested parties. The EAC will periodically assess the interpretations provided to determine which topics should be reflected in a future version of the *Guidelines*.

2 Description of the Technical Data Package

Table of Contents

2 Description of the Technical Data Package

2.1 Scope

This subsection contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition of national certification testing. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the vendor's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any information relevant to the system evaluation shall be submitted to include source code, object code, and sample output report formats.

Both formal documentation and notes of the vendor's system development process shall be submitted for qualification tests. Documentation describing the system development process permits assessment of the vendor's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. If the vendor's developmental test data are incomplete, the accredited test lab shall design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

2.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the system:

a. Overall system design, including subsystems, modules and the interfaces among them

b. Specific functional capabilities provided by the system

c. Performance and design specifications

d. Design constraints, applicable standards, and compatibility requirements

e. Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support

f. Vendor practices for assuring system quality during the system’s development and subsequent maintenance

g. Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle

The vendor shall provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the system. Documents shall be listed in order of precedence.

2.1.1.1 Required Content for Initial Certification

At minimum, the TDP shall contain the following documentation:

a. System configuration overview

b. System functionality description

c. System hardware specifications

d. Software design and specifications

e. System test and verification specifications

f. System security specifications

g. User/system operations procedures

h. System maintenance procedures

i. Personnel deployment and training requirements

j. Configuration management plan

k. Quality assurance program

l. System change notes

2.1.1.2 Required Content for System Changes and Re-certification

For systems seeking re-certification, vendors shall submit System Change Notes as described in Subsection 2.13, as well as current versions of all documents that have been updated to reflect system changes.

Vendors may also submit other information relevant to the evaluation of the system, such as test documentation, and records of the system's performance history, failure analysis and corrective actions.

2.1.1.3 Format

The requirements for formatting the TDP are general in nature; specific format details are of the vendor's choosing. The TDP shall include a detailed table of contents for the required documents, an abstract of each document and a listing of each of the informational sections and appendices presented. A cross-index shall be provided indicating the portions of the documents that are responsive to documentation requirements for any item presented.

2.1.2 Other Uses for Documentation

Although all of the TDP documentation is required for national certification testing, some of these same items may also be required during the state certification process and local level acceptance testing. Therefore, it is recommended that the technical documentation required for certification and acceptance testing be deposited in escrow.

2.1.3 Protection of Proprietary Information

The vendor shall identify all documents, or portions of documents, containing proprietary information not approved for public release. Any person or accredited test lab receiving proprietary information shall agree to use it solely for the purpose of analyzing and testing the system, and shall agree to refrain from otherwise using the proprietary information or disclosing it to any other person or agency without the prior written consent of the vendor, unless disclosure is legally compelled.

2.2 System Overview

In the system overview, the vendor shall provide information that enables the accredited test lab to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

2.2.1 System Description

The system description shall include written descriptions, drawings and diagrams that present:

a. A description of the functional components (or subsystems) as defined by the vendor (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships)

b. A description of the operational environment of the system that provides an overview of the hardware, software, and communications structure

c. A concept of operations that explains each system function, and how the function is achieved in the design

d. Descriptions of the functional and physical interfaces between subsystems and components

e. Identification of all COTS hardware and software products and communications services used in the development and/or operation of the voting system, identifying the name, vendor, and version used for each such component, including:

    i. Operating systems

    ii. Database software

    iii. Communications routers

    iv. Modem drivers

    v. Dial-up networking software

f. Interfaces among internal components, and interfaces with external systems. For components that interface with other components for which multiple products may be used, the TDP shall provide an identification of:

    i. File specifications, data objects, or other means used for information exchange

    ii. The public standard used for such file specifications, data objects, or other means

g. Benchmark directory listings for all software (including firmware elements) and associated documentation included in the vendor's release in the order in which each piece of software would normally be installed upon system setup and installation

2.2.2 System Performance

The vendor shall provide system performance information including:

a. The performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency

b. Quality attributes such as reliability, maintainability, availability, usability, and portability

c. Provisions for safety, security, privacy, and continuity of operation

d. Design constraints, applicable standards, and compatibility requirements

2.3 System Functionality Description

The vendor shall declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system.

The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Guidelines and any additional capabilities provided by the system. This listing shall provide a simple description of each capability. Detailed specifications shall be provided in other documentation required for the TDP.

a. The vendor shall organize the presentation of required capabilities in a manner that corresponds to the structure and sequence of functional capabilities indicated in Volume I, Section 2. The contents of Volume I, Section 2 may be used as the basis for a checklist to indicate the specific functions provided and those not provided by the system

b. Additional capabilities shall be clearly indicated. They may be presented using the same structure as that used for required capabilities (i.e., overall system capabilities, pre-voting functions, voting functions, post-voting functions), or may be presented in another format of the vendor's choosing

c. Required capabilities that may be bypassed or deactivated during installation or operation by the user shall be clearly indicated

d. Additional capabilities that function only when activated during installation or operation by the user shall be clearly indicated

e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user shall be clearly indicated

2.4 System Hardware Specification

The vendor shall expand on the system overview by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.

2.4.1 System Hardware Characteristics

The vendor shall provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in Volume I, Section 4, including:

Performance characteristics: This discussion addresses basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance

Physical characteristics: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors

Reliability: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability

Maintainability: Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability also addresses a range of scheduled and unscheduled events

Environmental conditions: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system

2.4.2 Design and Construction

The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole. Paragraphs and diagrams shall be provided that describe:

a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification

b. The electromagnetic environment generated by the system

c. Operator and voter safety considerations, and any constraints on system operations or the use environment

d. Human factors considerations, including provisions for access by disabled voters

2.5 Software Design and Specification

The vendor shall expand on the system overview by providing detailed specifications of the software components of the system, including software used to support the telecommunications capabilities of the system, if applicable.

2.5.1 Purpose and Scope

The vendor shall describe the function or functions that are performed by the software programs that comprise the system, including software used to support the telecommunications capabilities of the system, if applicable.

2.5.2 Applicable Documents

The vendor shall list all documents controlling the development of the software and its specifications. Documents shall be listed in order of precedence.

2.5.3 Software Overview

The vendor shall provide an overview of the software that includes the following items:

a. A description of the software system concept, including specific software design objectives, and the logic structure and algorithms used to accomplish these objectives

b. The general design, operational considerations, and constraints influencing the design of the software

c. Identification of all software items, indicating items that were:

   i. Written in-house

   ii. Procured and not modified

   iii. Procured and modified, including descriptions of the modifications to the software and to the default configuration options

d. Additional information for each item that includes:

   i. Item identification

   ii. General description

   iii. Software requirements performed by the item

iv. Identification of interfaces with other items that provide data to, or receive data from, the item

v. Concept of execution for the item

The vendor shall also include a certification that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

2.5.4 Software Standards and Conventions

The vendor shall provide information that can be used by an accredited test lab or state certification board to support software analysis and test design. The information shall address standards and conventions developed internally by the vendor as well as published industry standards that have been applied by the vendor. The vendor shall provide information that addresses the following standards and conventions:

a. Software System development methodology

b. Software design standards, including internal vendor procedures

c. Software specification standards, including internal vendor procedures

d. Software coding standards, including internal vendor procedures

e. Testing and verification standards, including internal vendor procedures, that can assist in determining the program's correctness and ACCEPT/REJECT criteria

f. Quality assurance standards or other documents that can be used to examine and test the software. These documents include standards for program flow and control charts, program documentation, test planning, and test data acquisition and reporting

2.5.5 Software Operating Environment

This section shall describe or make reference to all operating environment factors that influence the software design.

2.5.5.1 Hardware Environment and Constraints

The vendor shall identify and describe the hardware characteristics that influence the design of the software, such as:

a. The logic and arithmetic capability of the processor

b. Memory read-write characteristics

c. External memory device characteristics

d. Peripheral device interface hardware

e. Data input/output device protocols

f. Operator controls, indicators, and displays

2.5.5.2 Software Environment

The vendor shall identify the compilers or assemblers used in the generation of executable code, and describe the operating system or system monitor.

2.5.6 Software Functional Specification

The vendor shall provide a description of the operating modes of the system and of software capabilities to perform specific functions.

2.5.6.1 Configurations and Operating Modes

The vendor shall describe all software configurations and operating modes of the system, such as ballot preparation, election programming, preparation for opening the polling place, recording votes and/or counting ballots, closing the polling place, and generating reports. For each software function or operating mode, the vendor shall provide:

a. A definition of the inputs to the function or mode (with characteristics, tolerances or acceptable ranges, as applicable)

b. An explanation of how the inputs are processed

c. A definition of the outputs produced (again, with characteristics, tolerances, or acceptable ranges, as applicable)

2.5.6.2 Software Functions

The vendor shall describe the software's capabilities or methods for detecting or handling:

a. Exception conditions

b. System failures

c. Data input/output errors

d. Error logging for audit record generation

e. Production of statistical ballot data

f. Data quality assessment

g. Security monitoring and control

2.5.7 Programming Specifications

The vendor shall provide in this section an overview of the software design, its structure, and implementation algorithms and detailed specifications for individual software modules.

2.5.7.1 Programming Specifications Overview

This overview shall include such items as flowcharts, data flow diagrams, and other graphical techniques that facilitate understanding of the programming specifications. This section shall be prepared to facilitate understanding of the internal functioning of the individual software modules. Implementation of the functions shall be described in terms of the software architecture, algorithms, and data structures.

2.5.7.2 Programming Specifications Details

The programming specifications shall describe individual software modules and their component units, if applicable. For each module and unit, the vendor shall provide the following information:

a. Module and unit design decisions, if any, such as algorithms used

b. Any constraints, limitations, or unusual features in the design of the software module or unit

c. The programming language used and rationale for its use, if other than the specified module or unit language

d. If the software module or unit consists of, or contains, procedural commands (such as menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), a list of the procedural commands and reference to user manuals or other documents that explain them

e. If the software module or unit contains, receives, or outputs data, a description of its inputs, outputs, and other data elements as applicable. (Subsection 2.5.9 describes the

requirements for documenting system interfaces.) Data local to the software module or unit shall be described separately from data input to, or output from, the software module or unit

f. If the software module or unit contains logic, the logic to be used by the software unit, including, as applicable:

    i. Conditions in effect within the software module or unit when its execution is initiated

    ii. Conditions under which control is passed to other software modules or units

    iii. Response and response time to each input, including data conversion, renaming, and data transfer operations

    iv. Sequence of operations and dynamically controlled sequencing during the software module's or unit's operation, including:

        - The method for sequence control
        - The logic and input conditions of that method, such as timing variations, priority assignments
        - Data transfer in and out of memory
        - The sensing of discrete input signals, and timing relationships between interrupt operations within the software module or unit

g. Exception and error handling

h. If the software module is a database, provide the information described in Subsection 2.5.8

2.5.8 System Database

The vendor shall identify and provide a diagram and narrative description of the system's databases, and any external files used for data input or output. The information provided shall include for each database or external file:

a. The number of levels of design and the names of those levels (such as conceptual, internal, logical, and physical)

b. Design conventions and standards (which may be incorporated by reference) needed to understand the design

c. Identification and description of all database entities and how they are implemented physically (e.g., tables, files)

d. Entity relationship diagrams and description of relationships

e. Details of table, record or file contents (as applicable) to include individual data elements and their specifications, including:

   i. Names/identifiers

   ii. Data type (alphanumeric, integer, etc.)

   iii. Size and format (such as length and punctuation of a character string)

   iv. Units of measurement (such as meters, dollars, nanoseconds)

   v. Range or enumeration of possible values (such as 0-99)

   vi. Accuracy (how correct) and precision (number of significant digits)

   vii. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply

   viii. Security and privacy constraints

   ix. Sources (setting/sending entities) and recipients (using/receiving entities)

f. For external files, a description of the procedures for file maintenance, management of access privileges, and security

2.5.9 Interfaces

The vendor shall identify and provide a complete description of all internal and external interfaces, using a combination of text and diagrams.

2.5.9.1 Interface Identification

For each interface identified in the system overview, the vendor shall:

a. Provide a unique identifier assigned to the interface

b. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable

c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed on them)

2.5.9.2 Interface Description

For each interface identified in the system overview, the vendor shall provide information that describes:

a. The type of interface (such as real-time data transfer, storage-and-retrieval of data) to be implemented

b. Characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

   i. Names/identifiers

   ii. Data type (alphanumeric, integer, etc.)

   iii. Size and format (such as length and punctuation of a character string)

   iv. Units of measurement (such as meters, dollars, nanoseconds)

   v. Range or enumeration of possible values (such as 0-99)

   vi. Accuracy (how correct) and precision (number of significant digits)

   vii. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply

   viii. Security and privacy constraints

   ix. Sources (setting/sending entities) and recipients (using/receiving entities)

c. Characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:

   i. Communication links/bands/frequencies/media and their characteristics

   ii. Message formatting

   iii. Flow control (such as sequence numbering and buffer allocation)

   iv. Data transfer rate, whether periodic/aperiodic, and interval between transfers

   v. Routing, addressing, and naming conventions

   vi. Transmission services, including priority and grade

   vii. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing

d. Characteristics of protocols the interfacing entity(ies) will use for the interface, such as:

    i. Priority/layer of the protocol

    ii. Packeting, including fragmentation and reassembly, routing, and addressing

    iii. Legality checks, error control, and recovery procedures

    iv. Synchronization, including connection establishment, maintenance, termination

    v. Status, identification, and any other reporting features

e. Other characteristics, such as physical compatibility of the interfacing entity(ies) (such as dimensions, tolerances, loads, voltages and plug compatibility)

2.5.10 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the Software Specifications. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendix form include:

Glossary: A listing and brief definition of all software module names and variable names, with reference to their locations in the software structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used in an unorthodox semantic

References: A list of references to all related vendor documents, data, standards, and technical sources used in software development and testing

Program Analysis: The results of software configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final software design and coding

2.6 System Security Specification

Vendors shall submit a system security specification that addresses the security requirements of Volume I, Section 7. This specification shall describe the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks as defined in Volume I, Section 6, the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.

Information provided by the vendor in this section of the TDP may be duplicative of information required by other sections. Vendors may cross reference to information provided in other sections provided that the means used provides a clear mapping to the requirements of this section.

Information submitted by the vendor shall be used to assist in developing and executing the system certification test plan. The Security Specification shall contain the sections identified below.

2.6.1 Access Control Policy

The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective voting system security. The access control policy shall address the general features and capabilities and individual access privileges indicated in Volume I, Subsection 7.2.

2.6.2 Access Control Measures

The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access to meet the specific requirements of Volume I, Subsection 7.2.

The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.

2.6.3 Equipment and Data Security

The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data to meet the specific requirements of Volume I, Subsection 7.3. This information shall address measures for polling place security and central count location security.

2.6.4 Software Installation

The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements of Volume I, Subsection 7.4. This information shall address software installation for all system components.

2.6.5 Telecommunications and Data Transmission Security

The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission to meet the specific requirements of Volume I, Subsection 7.5:

a. For all systems, this information shall address access control, and prevention of data interception

b. For systems that use public communications networks as defined in Volume I, Section 6, this information shall also include:

   i. Capabilities used to provide protection against threats to third party products and services

   ii. Policies and processes used by the vendor to ensure that such protection is updated to remain effective over time

   iii. Policies and procedures used by the vendor to ensure that current versions of such capabilities are distributed to user jurisdictions and are installed effectively by the jurisdiction

   iv. A detailed description of the system capabilities and procedures to be employed by the jurisdiction to diagnose the occurrence of a denial of service attack, to use an alternate method of voting, to determine when it is appropriate to resume voting over the network, and to consolidate votes cast using the alternate method

   v. A detailed description of all activities to be performed in setting up the system for operation that are mandatory to ensure effective system security, including testing of security before an election

   vi. A detailed description of all activities that should be prohibited during system setup and during the timeframe for voting operations, including both the hours when polls are open and when polls are closed

2.6.6 Other Elements of an Effective Security Program

The vendor shall provide a detailed description of the following additional procedures required for use by the purchasing jurisdiction:

a. Administrative and management controls for the voting system and election management, including access controls

b. Internal security procedures, including operating procedures for maintaining the security of the software for each system function and operating mode

c. Adherence to, and enforcement of, operational procedures (e.g., effective password management)

d. Physical facilities and arrangements

e. Organizational responsibilities and personnel screening

This documentation shall be prepared such that these requirements can be integrated by the jurisdiction into local administrative and operating procedures.

2.7 System Test and Verification Specification

The vendor shall provide test and verification specifications for:

a. Development test specifications

b. National certification test specifications

2.7.1 Development Test Specifications

The vendor shall describe the plans, procedures, and data used during software development and system integration to verify system logic correctness, data quality, and security. This description shall include:

a. Test identification and design, including:

i. Test structure

ii. Test sequence or progression

iii. Test conditions

b. Standard test procedures, including any assumptions or constraints

c. Special purpose test procedures including any assumptions or constraints

d. Test data; including the data source, whether it is real or simulated, and how test data are controlled

e. Expected test results

f. Criteria for evaluating test results

Additional details for these requirements are provided by MIL-STD-498, Software Test Plan and Software Test Description. In the event that test data are not available, the accredited test

lab shall design test cases and procedures equivalent to those ordinarily used during product verification.

2.7.2 National Certification Test Specifications

The vendor shall provide specifications for verification and validation of overall software performance. These specifications shall cover:

a. Control and data input/output

b. Acceptance criteria

c. Processing accuracy

d. Data quality assessment and maintenance

e. Ballot interpretation logic

f. Exception handling

g. Security

h. Production of audit trails and statistical data

The specifications shall identify procedures for assessing and demonstrating the suitability of the software for election use.

2.8 System Operations Procedures

This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Subsection 2.3 above. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

The system operations procedures shall contain all information that is required for the preparation of detailed system operating procedures, and for operator training, as described below.

2.8.1 Introduction

The vendor shall provide a summary of system operating functions and modes, in sufficient detail to permit understanding of the system's capabilities and constraints. The roles of

operating personnel shall be identified and related to the operating modes of the system. Decision criteria and conditional operator functions (such as error and failure recovery actions) shall be described.

The vendor shall also list all reference and supporting documents pertaining to the use of the system during election operations.

2.8.2 Operational Environment

The vendor shall describe the system environment, and the interface between the user or operator and the system. The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

a. Polling place

b. Central count facility

c. Other locations

2.8.3 System Installation and Test Specification

The vendor shall provide specifications for validation of system installation, acceptance, and readiness. These specifications shall address all components of the system and all locations of installation (e.g., polling place, central count facility), and shall address all elements of system functionality and operations identified in Subsection 2.3 above, including:

a. Pre-voting functions

b. Voting functions

c. Post-voting functions

d. General capabilities

These specifications also serve to provide guidance to the procuring agency in developing its acceptance test plan and procedures according to the agency's contract provisions, and the election laws of the state.

2.8.4 Operational Features

The vendor shall provide documentation of system operating features that meets the following requirements:

a. A detailed description of all input, output, control, and display features accessible to the operator or voter

b. Examples of simulated interactions to facilitate understanding of the system and its capabilities

c. Sample data formats and output reports

d. Illustrate and describe all status indicators and information messages

2.8.5 Operating Procedures

The vendor shall provide documentation of system operating procedures that meets the following requirements:

a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation

b. Provides procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages)

c. Provides procedures that clearly enable the operator to intervene in system operations to recover from an abnormal system state

d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system

e. Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also shall be provided for the interaction of the system with other data processing systems or data interchange protocols

f. Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail

g. Supports successful ballot and program installation and control by election officials, provides a detailed work plan or other form of documentation providing a schedule and steps for the software and ballot installation, which includes a table outlining the key dates, events and deliverables

h. Supports diagnostic testing, specifies diagnostic tests that may be employed to identify problems in the system, verifies the correction of maintenance problems; and isolates and diagnoses faults from various system states

2.8.6 Operations Support

The vendor shall provide documentation of system operating procedures that meets the following requirements:

a. Defines the procedures required to support system acquisition, installation, and readiness testing. These procedures may be provided by reference, if they are contained either in the system hardware specifications, or in other vendor documentation

b. Describes procedures for providing technical support, system maintenance and correction of defects, and for incorporating hardware upgrades and new software releases

2.8.7 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Operations Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for discussion include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer operations

References: A list of references to all vendor documents and to other sources related to operation of the system

Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; Alternative procedures may be specified depending on the system state

Manufacturer's Recommended Security Procedures: This appendix shall contain the security procedures that are to be executed by the system operator

2.9 System Maintenance Manual

The system maintenance procedures shall provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required.

Recommended service actions to correct malfunctions or problems shall be discussed, along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include the sections listed below.

2.9.1 Introduction

The vendor shall describe the structure and function of the equipment (and related software) for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance, and for identification of faulty hardware or software. The description shall include a concept of operations that fully describes such items as:

a. The electrical and mechanical functions of the equipment

b. How the processes of ballot handling and reading are performed (paper-based systems)

c. How vote selection and casting of the ballot are performed (DRE systems);

d. How transmission of data over a network is performed (DRE systems, where applicable)

e. How data are handled in the processor and memory units

f. How data output is initiated and controlled

g. How power is converted or conditioned

h. How test and diagnostic information is acquired and used

2.9.2 Maintenance Procedures

The vendor shall describe preventive and corrective maintenance procedures for hardware and software.

2.9.2.1 Preventive Maintenance Procedures

The vendor shall identify and describe:

a. All required and recommended preventive maintenance tasks, including software tasks such as software backup, database performance analysis, and database tuning

b. Number and skill levels of personnel required for each task

c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance

d. Any maintenance tasks that must be coordinated with the vendor or a third party (such as coordination that may be needed for off-the-shelf items used in the system)

2.9.2.2 Corrective Maintenance Procedures

The vendor shall provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

The vendor shall identify specific procedures to be used in diagnosing and correcting problems in the system hardware (or user-controlled software). Descriptions shall include:

a. Steps to replace failed or deficient equipment

b. Steps to correct deficiencies or faulty operations in software

c. Modifications that are necessary to coordinate any modified or upgraded software with other software modules

d. The number and skill levels of personnel needed to accomplish each procedure

e. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure

f. Any coordination required with the vendor, or other party, for off the shelf items

2.9.3 Maintenance Equipment

The vendor shall identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

2.9.4 Parts and Materials

Vendors shall provide detailed documentation of parts and materials needed to operate and maintain the system. Additional requirements apply for paper-based systems.

2.9.4.1 Common Standards

The vendor shall provide a complete list of approved parts and materials needed for maintenance. This list shall contain sufficient descriptive information to identify all parts by:

a. Type

b. Size

c. Value or range

d. Manufacturer's designation

e. Individual quantities needed

f. Sources from which they may be obtained

2.9.4.2 Paper-based Systems

For marking devices manufactured by multiple external sources, the vendor shall provide a listing of sources and model numbers that are compatible with the system.

The TDP shall specify the required paper stock, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size and location of punch or mark fields used for vote response fields and to identify unique ballot formats, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

2.9.5 Maintenance Facilities and Support

The vendor shall identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance. In addition, vendors shall specify the assumptions made with regard to any parameters that impact the mean time to repair. These factors shall include at a minimum:

a. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation

b. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation

c. Organizational affiliation (i.e., jurisdiction, vendor) of qualified maintenance personnel

2.9.6 Appendices

The vendor may provide descriptive material and data supplementing the various sections of the body of the System Maintenance Manual. The content and arrangement of appendices shall be at the discretion of the vendor. Topics recommended for amplification or treatment in appendices include:

Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either voting systems or computer maintenance

References: A list of references to all vendor documents and other sources related to maintenance of the system

Detailed Examples: Detailed scenarios that outline correct system responses to every conceivable faulty operator input; alternative procedures may be specified depending on the system state

Maintenance and Security Procedures: This appendix shall contain technical illustrations and schematic representations of electronic circuits unique to the system

2.10 Personnel Deployment and Training Requirements

The vendor shall describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

2.10.1 Personnel

The vendor shall specify the number of personnel and skill levels required to perform each of the following functions:

a. Pre-election or election preparation functions (e.g., entering an election, contest and candidate information; designing a ballot; generating pre-election reports

b. System operations for voting system functions performed at the polling place

c. System operations for voting system functions performed at the central count facility

d. Preventive maintenance tasks

e. Diagnosis of faulty hardware or software

f. Corrective maintenance tasks

g. Testing to verify the correction of problems

A description shall be presented of which functions may be carried out by user personnel, and those that must be performed by vendor personnel.

2.10.2 Training

The vendor shall specify requirements for the orientation and training of the following personnel:

a. Poll workers supporting polling place operations

b. System support personnel involved in election programming

c. User system maintenance technicians

d. Network/system administration personnel (if a network is used)

e. Information systems personnel

f. Vendor personnel

2.11 Configuration Management Plan

Vendors shall submit a Configuration Management Plan that addresses the configuration management requirements of Volume I, Section 9. This plan shall describe all policies, processes, and procedures employed by the vendor to carry out these requirements. Information submitted by the vendor shall be used by the accredited test lab to assist in developing and executing the system certification test plan. This information is particularly important to support the design of test plans for system modifications. A well-organized, robust and detailed Configuration Management Plan will enable the accredited test lab to more readily determine the nature and scope of tests needed to fully test the modifications. The Configuration Management Plan shall contain the sections identified below.

2.11.1 Configuration Management Policy

The vendor shall provide a description of its organizational policies for configuration management, addressing the specific requirements of Volume I, Subsection 9.2. These requirements pertain to:

a. Scope and nature of configuration management program activities

b. Breadth of application of vendor's policy and practices to the voting system

2.11.2 Configuration Identification

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.3. These requirements pertain to:

a. Classifying configuration items into categories and subcategories

b. Uniquely numbering or otherwise identifying configuration items

c. Naming configuration items

2.11.3 Baseline and Promotion

The vendor shall provide a description of the procedures and naming conventions used to address the specific requirements of Volume I, Subsection 9.4. These requirements pertain to:

a. Establishing a particular instance of a system component as the starting baseline

b. Promoting subsequent instances of a component to baseline throughout the system development process for the first complete version of the system submitted for testing

c. Promoting subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained)

2.11.4 Configuration Control Procedures

The vendor shall provide a description of the procedures used by the vendor to approve and implement changes to a configuration item to prevent unauthorized additions, changes, or deletions to address the specific requirements of Volume I, Subsection 9.5. These requirements pertain to:

a. Developing and maintaining internally developed items

b. Developing and maintaining third party items

c. Resolving internally identified defects

d. Resolving externally identified and reported defects

2.11.5 Release Process

The vendor shall provide a description of the contents of a system release, and the procedures and related conventions by which the vendor installs, transfers, or migrates the system to accredited voting system testing laboratories and customers to address the specific requirements of Volume I, Subsection 9.6. These requirements pertain to:

a. A first release of the system to an accredited test lab

b. A subsequent maintenance or upgrade release of a system, or particular components, to an accredited test lab

c. The initial delivery and installation of the system to a customer

d. A subsequent maintenance or upgrade release of a system, or particular components, to a customer

2.11.6 Configuration Audits

The vendor shall provide a description of the procedures and related conventions for the two audits required by Volume I, Subsection 9.7. These requirements pertain to:

a. Physical configuration audit that verifies the voting system components submitted for certification testing to the vendor's technical documentation

b. Functional configuration audit that verifies the system performs all the functions described in the system documentation

2.11.7 Configuration Management Resources

The vendor shall provide a description of the procedures and related conventions for maintaining information about configuration management tools required by Volume I, Subsection 9.8. These requirements pertain to information regarding:

a. Specific tools used, current version, and operating environment

b. Physical location of the tools, including designation of computer directories and files

c. Procedures and training materials for using the tools

2.12 Quality Assurance Program

Vendors shall submit a Quality Assurance Program that addresses the quality assurance requirements of Volume I, Section 8. This plan shall describe all policies, processes, and procedures employed by the vendor to ensure the overall quality of the system for its initial development and release and for subsequent modifications and releases. This information is particularly important to support the design of test plans by the accredited test lab. A well-organized, robust and detailed Quality Assurance Program will enable the accredited test lab to more readily determine the nature and scope of tests needed to test the system appropriately. The Quality Assurance Program shall, at a minimum, address the topics indicated below.

2.12.1 Quality Assurance Policy

The vendor shall provide a description of its organizational policies for quality assurance, including:

a. Scope and nature of Quality Assurance activities

b. Breadth of application of vendor's policy and practices to the voting system

2.12.2 Parts and Materials Tests

The vendor shall provide a description of its practices for parts and materials tests and examinations that meet the requirements of Volume I, Subsection 8.5.

2.12.3 Quality Conformance Inspections

The vendor shall provide a description of its practices for quality conformance inspections that meet the requirements of Volume I, Subsection 8.6. For each test performed, the record of tests provided shall include:

a. Test location

b. Test date

c. Individual who conducted the test

d. Test outcomes

2.12.4 Documentation

The vendor shall provide a description of its practices for documentation of the system and system development process that meet the requirements of Volume I, Subsection 8.7.

2.13 System Change Notes

Vendors submitting modifications for a system that has been tested previously and received national certification shall submit system change notes. These will be used by the accredited test lab to assist in developing and executing the test plan for the modified system. The system change notes shall include the following information:

a. Summary description of the nature and scope of the changes, and reasons for each change

b. A listing of the specific changes made, citing the specific system configuration items changed and providing detailed references to the documentation sections changed

c. The specific sections of the documentation that are changed (or completely revised documents, if more suitable to address a large number of changes)

d. Documentation of the test plan and procedures executed by the vendor for testing the individual changes and the system as a whole, and records of test results

3 Functionality Testing

Table of Contents

3 Functionality Testing

3.1 Scope

This section contains a description of the testing to be performed to confirm the functional capabilities of a voting system submitted for national certification. It describes the scope and basis for functionality testing, outlines the general sequence of tests within the overall test process, and provides guidance on testing for accessibility.

3.2 Breadth of Functionality Testing

In order to best complement the diversity of the voting systems industry, the certification testing process is not rigidly defined. Although there are basic functionality testing requirements, additions or variations in testing are appropriate to the use of specific technologies and configurations, system capabilities, and the outcomes of previous testing.

3.2.1 Basic Functionality Testing Requirements

The accredited test lab shall design and perform procedures to test a voting system against the functional requirements outlined in Volume I, Section 2. Test procedures shall be designed and performed that address:

a. Overall system capabilities

b. Pre-voting functions

c. Voting functions

d. Post-voting functions

e. System maintenance

f. Transportation and storage

The specific procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for independent functionality testing.

Recognizing variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for such variations and reflect the system-specific functional capabilities in Volume I, Section 2.

3.2.2 Testing to Reflect Technologies

Voting systems are not designed according to a standard design template. Instead, system design reflects the vendor's selections from a variety of technologies and design configurations. Such variation is recognized in the definitions of voting systems in Volume I, Section 1, and serves as the basis for delineating various functional capability requirements.

Functional capabilities will vary according to the relative complexity of a system and the manner in which the system integrates various technologies. Therefore, the testing procedure designed and performed for a particular system shall reflect the specific technologies and design configurations used by that system.

3.2.3 Testing to Reflect Additional Capabilities

The requirements for voting system functionality provided by Volume I, Section 2 reflect a minimum set of capabilities. Vendors may, and often do, provide additional capabilities in systems in order to respond to the requirements of individual states. These additional capabilities shall be identified by the vendor within the TDP, as described in Volume II, Section 2. Based on this information, the accredited test lab shall design and perform system functionality testing for these additional functional capabilities.

3.2.4 Testing to Reflect Previously Tested Capabilities

The required functional capabilities of voting systems defined in Volume I, Section 2 reflect a broad range of system functionality needed to support the full life cycle of an election, including post election activities. Many systems submitted for certification are designed to address this scope, and are to be tested accordingly.

However, some new systems using a combination of new subsystems or system components interfaced with the components of a previously certified system. For example, a vendor can submit a voting system certification testing that has a new DRE voting device, but that integrates the election management component from a previously certified system.

In this situation, the vendor shall identify in the TDP the functional capabilities supported by new subsystems/components and those supported by subsystems/components taken from a previously certified system. The vendor shall indicate in its system design documentation and configuration management records the scope and nature of any modifications made to the re-used subsystems or components. This will assist the accredited test lab to develop efficient test procedures that rely in part on the results of testing of the previously certified subsystems or components.

In this situation the accredited test lab may design and perform a test procedure that draws on the results of testing performed previously on re-used subsystems or components. However,

irrespective of previous testing performed, the scope of testing shall include certain functionality tests:

a. All functionality performed by new subsystems/modules

b. All functionality performed by modified subsystems/modules

c. Functionality that is accomplished using any interfaces to new modules, or that shares inputs or outputs from new modules

d. All functionality related to vote tabulation and election results reporting

e. All functionality related to audit trail maintenance

3.3 General Test Sequence

There is no required sequence for performing the system certification tests. For a system not previously certified, the accredited test lab may perform tests using generic test ballots, and schedule the tests in a convenient order, provided that prerequisite conditions for each test have been satisfied before the test is initiated.

Regardless of the sequence of testing used, the full certification testing process shall include functionality testing for all system functions of a voting system. Generally, in depth functionality testing will follow testing of the system hardware and the source code review of the software. The accredited test lab will usually conduct functionality testing as an integral element of the system integration testing described in Section 6.

Some functionality tests for the voting functions defined in Volume I, Section 2.may be performed as an integral part of hardware testing, enabling a more efficient testing process. Ballots processed and counted during hardware operating tests for precinct count and central count systems may serve to satisfy part of the functionality testing, provided that the ballots were cast using a test procedure that is equivalent to the procedures indicated below.

3.3.1 Testing in Parallel with Precinct Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures shall be performed during the functionality tests of voting equipment and precinct counting equipment.

a. The procedure to prepare election programs shall:

   i. Verify resident firmware, if any

   ii. Prepare software (including firmware) to simulate all ballot format and logic options for which the system will be used

iii. Verify program memory device content

iv. Obtain and design test ballots with formats and voting patterns sufficient to verify performance of the test election programs

b. The procedures to program precinct ballot counters shall:

i. Install program and data memory devices, or verify presence if resident

ii. Verify operational status of hardware as specified in Volume II, Section 4

c. The procedures to simulate opening of the polls shall:

i. Perform procedures required to prepare hardware for election operations

ii. Obtain "zero" printout or other evidence that data memory has been cleared

iii. Verify audit log of pre-election operations

iv. Perform procedure required to open the polling place and enable ballot counting

d. The procedure to simulate counting ballots shall cast test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 5

e. The procedure to simulate closing of polls shall:

i. Perform hardware operations required to disable ballot counting and close the polls

ii. Obtain data reports and verify correctness

iii. Obtain audit log and verify correctness

These procedures need not be performed in the sequence listed, provided the necessary precondition of each procedure has been met.

3.3.2 Testing in Parallel with Central Count Systems

For testing voting functions defined in Volume I, Sections 2, the following procedures shall be performed during the functional tests.

a. The procedure to prepare election programs shall:

i. Verify resident firmware, if any

ii. Prepare software (including firmware) to simulate all ballot format and logic

options for which the system will be used, and to enable simulation of counting ballots from at least 10 polling places or precincts

iii. Verify program memory device content

iv. Procure test ballots with formats, voting patterns, and format identifications sufficient to verify performance of the test election programs

b. The procedure to simulate counting ballots shall count test ballots in a number sufficient to demonstrate proper processing, error handling, and generation of audit data as specified in Volume I, Sections 2 and 5

c. The procedure to simulate election reports shall:

i. Obtain reports at polling places or precinct level

ii. Obtain consolidated reports

iii. Provide query access, if this is a feature of the system

iv. Verify correctness of all reports and queries

v. Obtain audit log and verify correctness

They need not be performed in the sequence listed, provided the necessary preconditions of each procedure have been met.

3.4 Functionality Testing for Accessibility

Volume I, Section 4 prescribes the requirements for voting system accessibility to satisfy the provisions of HAVA 301(a)(4) and 241(b)(5). To demonstrate conformance to these requirements, vendors shall conduct summative usability tests of accessible voting equipment with blind and visually impaired individuals and individuals lacking fine motor control. A description of the testing performed, the population of test subjects participating, and the results shall be documented using the Common Industry Format (CIF) by the vendor and submitted as part of the Technical Data Package. The test labs shall review this information during the system certification documentation review.

3.5 Testing for Systems that Operate on Personal Computers

For systems intended to use non-standard voting devices, such as a personal computer, provided by the local jurisdiction, the accredited test lab shall conduct functionality tests using hardware provided by the vendor that meets the minimum configuration specifications defined by the vendor.

Section 4 provides additional information on hardware to be used to conduct functionality testing of such voting devices, as well as hardware to be used to conduct security testing and other forms of testing.

4 Hardware Testing

Table of Contents

4 Hardware Testing

4.1 Scope

This section contains a description of the testing to be performed to confirm the proper functioning of the hardware components of a voting system. It describes the scope and basis for functionality testing, required test conditions for conducting hardware testing, guidance for the use of test fixtures, test log data requirements, and test practices for specific non-operating and operating environmental tests.

4.2 Basis of Hardware Testing

This section addresses the focus and applicability of hardware testing and specifies the vendor's obligations to produce hardware to conduct such tests.

4.2.1 Testing Focus and Applicability

The accredited test lab shall design and perform procedures that test the voting system hardware requirements identified in Volume I, Section 4. Test procedures shall be designed and performed for both operating and non-operating environmental tests:

a. Operating environmental tests apply to the entire system, including hardware components that are used as part of the voting system telecommunications capability

b. Non-operating tests apply to those elements of the system that are intended for use at poll site voting locations, such as voting machines and precinct counters. These tests address environmental conditions that may be encountered by the voting system hardware at the voting location itself, or while in storage or transit to or from the poll site

Additionally, compatibility of this equipment with the voting system environment shall be determined through functional tests integrating the standard product with the remainder of the system.

All hardware components that are custom-designed for election use shall be tested in accordance with the applicable procedures contained in this section. Unmodified COTS hardware will not be subject to all tests. Generally such equipment has been designed to rigorous industrial standards and has been in wide use, permitting an evaluation of its performance history. To enable reduced testing of such equipment, vendors shall provide the manufacturer specifications and evidence that the equipment has been tested to the equivalent of these Guidelines.

The specific testing procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for hardware testing performed by the accredited test lab.

4.2.2 Hardware Provided by Vendor

The hardware submitted for national certification testing shall be equivalent, in form and function, to the actual production versions of the hardware units. Engineering or developmental prototypes are not acceptable unless the vendor can show that the equipment to be tested is equivalent to standard production units in both performance and construction.

4.3 Test Conditions

Certification tests may be performed in any facility capable of supporting the test environment. Preparation for testing, arrangement of equipment, verification of equipment status, and the execution of procedures shall be witnessed by at least one independent, qualified observer who shall certify that all test and data acquisition requirements have been satisfied.

When a test is to be performed at "standard" or "ambient" conditions, this requirement shall refer to a nominal laboratory environment at prevailing atmospheric pressure and relative humidity.

Otherwise, all tests shall be performed at the required temperature and electrical supply voltage, regulated within the following tolerances:

a. Temperature of +/- 4 degrees F

b. Electrical supply voltage +/- 2 voltage alternating current

4.4 Test Log Data Requirements

The accredited test lab shall maintain a test log of the procedure employed. This log shall identify the system and equipment by model and serial number. Test environment conditions shall be noted.

In the event that the accredited test lab deems it necessary to deviate from requirements pertaining to the test environment, the equipment arrangement and method of operation, the specified test procedure, or the provision of test instrumentation and facilities, the deviation shall be recorded in the test log. A discussion of the reasons for the deviation and the effect of the deviation on the validity of the test procedure shall also be provided.

4.5 Test Fixtures

The use of test fixtures or ancillary devices to facilitate hardware testing is encouraged. These fixtures and devices may include arrangements for automating the operation of voting devices and the acquisition of test data.

The use of a fixture to ensure correctness in casting ballots by hand is recommended. Such a fixture may consist of a template, with apertures in the desired location, so that selections may be made rapidly. Such a template will eliminate or greatly minimize errors in activating test ballot patterns, while reducing the amount of time required to cast a test ballot.

For systems that use a light source as a means of detecting voter selections, the generation of a suitable optical signal by an external device is acceptable. For systems that rely on the physical activation of a switch, a mechanical fixture with suitable motion generators is acceptable.

To speed up the process of testing and to eliminate human error in casting test ballots the tests may use a simulation device with appropriate software. Such simulation is recommended if it covers all voting data detection and control paths that are used in casting an actual ballot. In the event that only partial simulation is achieved, then an independent method and test procedure must be used to validate the proper operation of those portions of the system not tested by the simulator.

If the vendor provides a means of simulating the casting of ballots, the simulation device is subject to the same performance, reliability, and quality requirements that apply to the voting device itself so as not to contribute errors to the test processes.

4.6 Non-operating Environmental Tests

This section addresses a range of tests for voting machines and precinct counters, as such devices are stored between elections and are transported between the storage facility and polling place.

4.6.1 General

Environmental tests of non-operating equipment are intended to simulate exposure to physical shock and vibration associated with handling and transportation of voting equipment and precinct counters between a jurisdiction's storage facility and precinct polling places. These tests additionally simulate the temperature and humidity conditions that may be encountered during storage in an uncontrolled warehouse environment or precinct environment. The procedures and conditions of these tests correspond generally to those of MIL-STD-810D, "Environmental Test Methods and Engineering Guidelines," 19 July 1983. In most cases, the severity of the test conditions has been reduced to reflect commercial, rather than military, practice.

Systems exclusively designed with system-level COTS hardware whose configuration has not been modified in any manner are not subject to this segment of hardware testing. Systems made up of individual COTS components such as hard drives, motherboards, and monitors that have been packaged to build a voting machine or other device will be required to undergo the hardware testing.

Prior to each test, the equipment shall be shown to be operational by means of the procedure contained in Subsection 4.6.1.5. The equipment may then be prepared as if for actual transportation or storage, and subjected to appropriate test procedures outlined. After each procedure has been completed, the equipment status will again be verified as in Subsection 4.6.1.5.

The following requirements for equipment preparation, functional tests, and inspections shall apply to each of the non-operating test procedures.

4.6.1.1 Pretest Data

The test technician shall verify that the equipment is capable of normal operation. Equipment identification, environmental conditions, equipment configuration, test instrumentation, operator tasks, time-of-day or test time, and test results shall be recorded.

4.6.1.2 Preparation for Test

The equipment shall be prepared as for the expected non-operating use, as noted below. When preparation for transport between the storage site and the polling place is required, the equipment shall be prepared with any protective enclosures or internal restraints that the vendor specifies for such transport. When preparation for storage is required, the equipment shall be prepared using any protective enclosures or internal restraints that the vendor specifies for storage.

4.6.1.3 Mechanical Inspection and Repair

After the test has been completed, the devices shall be removed from their containers, and any internal restraints shall be removed. The exterior and interior of the devices shall be inspected for evidence of mechanical damage, failure, or dislocation of internal components. Devices shall be adjusted or repaired, if necessary.

4.6.1.4 Electrical Inspection and Adjustment

After completion of the mechanical inspection and repair, routine electrical maintenance and adjustment may be performed, according to the manufacturer's standard procedure.

4.6.1.5 Operational Status Check

When all tests, inspections, repairs, and adjustments have been completed, normal operation shall be verified by conducting an operational status check.

During this process, all equipment shall be operated in a manner and under environmental conditions that simulate election use to verify the functional status of the system. Prior to the conduct of each of the environmental hardware non-operating tests, a supplemental test shall be made to determine that the operational state of the equipment is within acceptable performance limits.

The following procedures shall be followed to verify the equipment status:

Step 1: Arrange the system for normal operation.
Step 2: Turn on power, and allow the system to reach recommended operating temperature.
Step 3: Perform any servicing, and make any adjustments necessary, to achieve operational status.
Step 4: Operate the equipment in all modes, demonstrating all functions and features that would be used during election operations.
Step 5: Verify that all system functions have been correctly executed.

4.6.1.6 Failure Criteria

Upon completion of each non-operating test, the system hardware shall be subject to functional testing to verify continued operability. If any portion of the voting machine or precinct counter hardware fails to remain fully functional, the testing will be suspended until the failure is identified and corrected by the vendor. The system will then be subject to a retest.

4.6.2 Bench Handling Test

The bench handling test simulates stresses faced during maintenance and repair of voting machines and ballot counters.

4.6.2.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 516.3, Procedure VI.

4.6.2.2 Procedure

Step 1: Place each piece of equipment on a level floor or table, as for normal operation or servicing.
Step 2: Make provision, if necessary, to restrain lateral movement of the equipment or its supports at one edge of the device. Vertical rotation about that edge shall not be restrained.
Step 3: Using that edge as a pivot, raise the opposite edge to an angle of 45 degrees, to a height of four inches above the surface, or until the point of balance has been reached, whichever occurs first.
Step 4: Release the elevated edge so that it may drop to the test surface without restraint.
Step 5: Repeat steps 3 and 4 for a total of six events.
Step 6: Repeat steps 2, 3, and 4 for the other base edges, for a total of 24 drops for each device.

4.6.3 Vibration Test

The vibration test simulates stresses faced during transport of voting machines and ballot counters between storage locations and polling places.

4.6.3.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 514.3, Category 1- Basic Transportation, Common Carrier.

4.6.3.2 Procedure

Step 1: Install the test item in its transit or combination case as prepared for transport.
Step 2: Attach instrumentation as required to measure the applied excitation.
Step 3: Mount the equipment on a vibration table with the axis of excitation along the vertical axis of the equipment.
Step 4: Apply excitation as shown in MIL-STD-810D, Method 514.3-1, “Basic transportation, common carrier, vertical axis”, with low frequency excitation cutoff at 10 Hz, for a period of 30 minutes.
Step 5: Repeat steps 2 and 3 for the transverse and longitudinal axes of the equipment with the excitation profiles shown in Figures 514.3-2 and 514.3-3, respectively. (Note: The total excitation period equals 90 minutes, with 30 minutes excitation along each axis.)
Step 6: Remove the test item from its transit or combination case and verify its continued operability.

4.6.4 Low Temperature Test

The low temperature test simulates stresses faced during storage of voting machines and ballot counters.

4.6.4.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 502.2, Procedure I-Storage. The minimum temperature shall be -4 degrees F.

4.6.4.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2: Lower the internal temperature of the chamber at any convenient rate, but not so rapidly as to cause condensation in the chamber, and in any case no more rapidly than 10 degrees F per minute, until an internal temperature of -4 degrees F has been reached.
Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.
Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.
Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

4.6.5 High Temperature Test

The high temperature test simulates stresses faced during storage of voting machines and ballot counters.

4.6.5.1 Applicability

All systems and components, regardless of type, shall meet the requirements of this test. This test is equivalent to the procedure of MIL-STD-810D, Method 501.2, Procedure I-Storage. The maximum temperature shall be 140 degrees F.

4.6.5.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.

Step 2: Raise the internal temperature of the chamber at any convenient rate, but in any case no more rapidly than 10 degrees F per minute, until an internal temperature of 140 degrees F has been reached.
Step 3: Allow the chamber temperature to stabilize. Maintain this temperature for a period of 4 hours after stabilization.
Step 4: Allow the internal temperature of the chamber to return to standard laboratory conditions, at a rate not exceeding 10 degrees F per minute.
Step 5: Allow the internal temperature of the equipment to stabilize at laboratory conditions before removing it from the chamber.
Step 6: Remove the equipment from the chamber and from its containers, and inspect the equipment for evidence of damage.
Step 7: Verify continued operability of the equipment.

4.6.6 Humidity Test

The humidity test simulates stresses faced during storage of voting machines and ballot counters.

4.6.6.1 Applicability

All systems and components regardless of type shall meet the requirements of this test. This test is similar to the procedure of MIL-STD-810D, Method 507.2, Procedure I-Natural Hot-Humid. It is intended to evaluate the ability of the equipment to survive exposure to an uncontrolled temperature and humidity environment during storage. This test lasts for ten days.

4.6.6.2 Procedure

Step 1: Arrange the equipment as for storage. Install it in the test chamber.
Step 2 Adjust the chamber conditions to those given in MIL-STD-810D Table 507.2-I, for the time 0000 of the HotHumid cycle (Cycle 1).
Step 3: Perform a 24-hour cycle with the time and temperature-humidity values specified in Figure 507.2-1, Cycle 1.
Step 4: Repeat Step 2 until 5, 24-hour cycles have been completed.
Step 5: Continue with the test commencing with the conditions specified for time = 0000 hours.
Step 6: At any convenient time in the interval between time = 120 hours and time = 124 hours, place the equipment in an operational configuration, and perform a complete operational status check as defined in Subsection 4.6.1.5.
Step 7: If the equipment satisfactorily completes the status check, continue with the sixth 24-hour cycle.
Step 8: Perform 4 additional 24-hour cycles, terminating the test at time = 240 hours.
Step 9: Remove the equipment from the test chamber and inspect it for any evidence of damage.

Step 10: Verify continued operability of the equipment.

4.7 Environmental Tests, Operating

This section addresses a range of tests for all voting system equipment, including equipment for both precinct count and central count systems.

4.7.1 Temperature and Power Variation Tests

This test is similar to the low temperature and high temperature tests of MIL-STD-810-D, Method 502.2 and Method 501.2, with test conditions that correspond to the requirements of the performance standards. This procedure tests system operation under various environmental conditions for at least 163 hours. During 48 hours of this operating time, the device shall be in a test chamber. For the remaining hours, the equipment shall be operated at room temperature. The system shall be powered for the entire period of this test; the power may be disconnected only if necessary for removal of the system from the test chamber.

Operation shall consist of ballot-counting cycles, which vary with system type. An output report need not be generated after each counting cycle. The interval between reports, however, should be no more than 4 hours to keep to a practical minimum the time between the occurrence of a failure or data error and its detection.

Test Ballots per Counting Cycle	
Precinct count systems	100 ballots/hour
Central count systems	300 ballots/hour

The recommended pattern of votes is one chosen to facilitate visual recognition of the reported totals; this pattern shall exercise all possible voting locations. System features such as data quality tests, error logging, and audit reports shall be enabled during the test.

Each operating cycle shall consist of processing the number of ballots indicated above.

Step 1: Arrange the equipment in the test chamber. Connect as required and provide for power, control, and data service through enclosure wall.
Step 2: Set the supply voltage at 117 voltage alternating current.
Step 3: Power the equipment, and perform an operational status check as in Section 4.6.1.5.
Step 4: Set the chamber temperature to 50 degrees F, observing precautions against thermal shock and condensation.
Step 5: Begin 24 hour cycle.
Step 6: At T=4 hrs, lower the supply voltage to 105 vac.
Step 7: At T=8 hrs, raise the supply voltage to 129 vac.
Step 8: At T=11:30 hrs, return the supply voltage to 117 vac and return the chamber

temperature to lab ambient, observing precautions against thermal shock and condensation.

Step 9: At T=12:00 hrs, raise the chamber temperature to 95 degrees Fahrenheit.

Step 10: Repeat Steps 5 through 8, with temperature at 95 degrees Fahrenheit, complete at T=24 hrs.

Step 11: Set the chamber temperature at 50 degrees Fahrenheit as in Step 4.

Step 12: Repeat the 24 hour cycle as in Steps 5-10, complete at T=48 hrs.

Step 13: After completing the second 24 hour cycle, disconnect power from the system and remove it from the chamber if needed.

Step 14: Reconnect the system as in Step 2, and continue testing for the remaining period of operating time required until the ACCEPT/REJECT criteria of Subsection 4.7.1.1 have been met.

4.7.1.1 Data Accuracy

As indicated in Volume I, Section 4, data accuracy is defined in terms of ballot position error rate. This rate applies to the voting functions and supporting equipment that capture, record, store, consolidate, and report the specific selections, and absence of selections, made by the voter for each ballot position. Volume I, Subsection 4.1.1 identifies the specific functions to be tested.

For each processing function, the system shall achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions. This error rate includes errors from any source while testing a specific processing function and its related equipment.

This error rate is used to determine the vote position processing volume used to test system accuracy for each function:

a. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system

b. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted

c. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)

Appendix C provides further details of the calculation for this testing volume.

4.7.2 Maintainability Test

The accredited test lab shall test for maintainability based on the provisions of Volume I, Section 4 for maintainability, including both physical attributes and additional attributes regarding the ease of performing maintenance activities. These tests include:

a. Examining the physical attributes of the system to determine whether significant impediments exist for the performance of those maintenance activities that are to be performed by the jurisdiction. These activities shall be identified by the vendor in the system maintenance procedures portion of the TDP

b. Performing activities designated as maintenance activities for the jurisdiction in the TDP, in accordance with the instructions provided by the vendor in the system maintenance procedures, noting any difficulties encountered

Should significant impediments or difficulties be encountered that are not remedied by the vendor, the accredited test lab shall include such findings in the certification test results of the certification test report.

4.7.3 Reliability Test

The accredited test lab shall test for reliability based on the provisions of Volume I, Section 4 for the acceptable Mean Time Between Failure (MBTF). The MBTF shall be measured during the conduct of other system performance tests specified in this section, and shall be at least 163 hours. Appendix C provides further details of the calculation for this testing period.

4.7.4 Availability Test

The accredited test lab shall assess the adequacy of system availability based on the provisions of Volume I, Section 4. As described in this section, availability of voting system equipment is determined as a function of reliability, and the mean time to repair the system in the event of failure.

Availability cannot be tested directly before the voting system is deployed in jurisdictions, but can be modeled mathematically to predict availability for a defined system configuration. This model shall be prepared by the vendor, and shall be validated by the accredited testing laboratory.

The model shall reflect the equipment used for a typical system configuration to perform the following system functions:

a. For all paper-based systems:

    i. Recording voter selections (such as by ballot marking)

ii. Scanning the marks on paper ballots and converting them into digital data

b. For all DRE systems:

i. Recording and storing the voter's ballot selections

c. For precinct-count systems (paper-based and DRE):

i. Consolidation of vote selection data from multiple precinct-based systems to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

d. For central-count systems (paper-based and DRE):

i. Consolidation of vote selection data from multiple counting devices to generate jurisdiction-wide vote counts, including storage and reporting of the consolidated vote data

The model shall demonstrate the predicted availability of the equipment that supports each function. This demonstration shall reflect the equipment reliability, mean time to repair, and assumptions concerning equipment availability and deployment of maintenance personnel stated by the vendor in the TDP.

4.8 Other Environmental Tests

This section addresses a range of tests for all voting system equipment, including equipment for both precinct count and central count systems.

a. The test for power disturbance disruption shall be conducted in compliance with the test specified in IEC 61000-4-11 (1994-06).

b. The test for electromagnetic radiation shall be conducted in compliance with the FCC Part 15 Class B requirements by testing per ANSI C63.4.

c. The test for electrostatic disruption shall be conducted in compliance with the test specified in IEC 61000-4-2 (1995-01).

d. The test for electromagnetic susceptibility shall be conducted in compliance with the test specified in IEC 61000-4-3 (1996).

e. The test for electrical fast transient protection shall be conducted in compliance with the test specified in IEC 61000-4-4 (1995-01).

f. The test for lightning surge protection shall be conducted in compliance with the test specified in IEC 61000-4-5 (1995-02).

g. The test for conducted RF immunity shall be conducted in compliance with the test specified in IEC 61000-4-6 (1996-04).

h. The test for AC magnetic fields RF immunity shall be conducted in compliance with the test specified in IEC 61000-4-8 (1993-06).

5 Software Testing

Table of Contents

5 Software Testing

5.1 Scope

This section contains a description of the testing to be performed by the accredited test lab to confirm the proper functioning of the software components of a voting system submitted for certification testing. It describes the scope and basis for software testing, the initial review of documentation to support software testing, and the review of the voting system source code. Further testing of the voting system software is addressed in the following sections:

a. Section 3 for specific tests of voting system functionality

b. Section 6 for testing voting system security and for testing the operation of the voting system software together with other voting system components

5.2 Basis of Software Testing

The accredited test lab shall design and perform procedures that test the voting system software requirements identified in Volume I, Section 5. All software components designed or modified for election use shall be tested in accordance with the applicable procedures contained in this section.

Unmodified, general purpose COTS non-voting software (e.g., operating systems, programming language compilers, data base management systems, and Web browsers) is not subject to the detailed examinations specified in this section. However, the accredited test lab shall examine such software to confirm the specific version of software being used against the design specification to confirm that the software has not been modified. Portions of COTS software that have been modified by the vendor in any manner are subject to review.

Unmodified COTS software is not subject to code examination. However, source code generated by a COTS package and embedded in software modules for compilation or interpretation shall be provided in human readable form to the accredited test lab. The accredited test lab may inspect COTS source code units to determine testing requirements or to verify the code is unmodified.

The accredited test lab may inspect the COTS generated software source code in preparation of test plans and to provide some minimal scanning or sampling to check for embedded code or unauthorized changes. Otherwise, the COTS source code is not subject to the full code review and testing. For purposes of code analysis, the COTS units shall be treated as unexpanded macros.

Compatibility of the voting system software components or subsystems with one another, and with other components of the voting system environment, shall be determined through functional tests integrating the voting system software with the remainder of the system.

The specific procedures to be used shall be identified in the National Certification Test Plan prepared by the accredited test lab. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for software testing performed by the accredited test lab.

Recognizing the variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for these variations.

5.3 Initial Review of Documentation

Prior to initiating the software review, the accredited test lab shall verify that the documentation submitted by the vendor in the TDP is sufficient to enable:

a. Review of the source code

b. Design and conduct tests at every level of the software structure to verify that the software meets the vendor's design specifications and the requirements of the performance guidelines

5.4 Source Code Review

The accredited test lab shall compare the source code to the vendor's software design documentation to ascertain how completely the software conforms to the vendor's specifications. Source code inspection shall also assess the extent to which the code adheres to the requirements in Volume I, Section 5

5.4.1 Control Constructs

Voting system software shall use the control constructs identified in this section as follows:

a. If the programming language used does not provide these control constructs, the vendor shall provide them (that is, comparable control structure logic). The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution

b. While some programming languages do not create programs as linear processes, stepping from an initial condition, through changes, to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute

through these control constructs (or their equivalents, as defined and provided by the vendor)

c. Operator intervention or logic that evaluates received or stored data shall not re-direct program control within a program routine. Program control may be re-directed within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited

d. Conventional constructs that are inherent to the development language are permitted but must be documented in the code, adjacent to their use.

Illustrations of the following control construct techniques are provided in Figures 1 through 4.

a. Fig. 1 Sequence

b. Fig. 2 If -Then -Else

c. Fig. 3 Do -While

d. Fig. 4 Do -Until

e. Fig. 5 Case

f. Fig. 6 General loop, including the special case FOR loop

5.4.1.1 Replacement Rule

In the constructs shown, any ‘process’ may be replaced by a simple statement, a subroutine or function call, or any of the control constructs. In Fig 4-1 for example, “Process A” may be a simple statement and “Process B” another Sequence construct.

Using the replacement rule to replace one or both of the processes in the Sequence construct with other Sequence constructs, a large block of sequential code may be formed. The entire chain is recognized as a Sequence construct and is sometimes called a BLOCK construct. In many languages, a Sequence may need to be marked with special symbols or punctuation to delimit where it starts and where it ends. For example, a “BEGIN” and “END” may be used. This allows the scope of a Sequence used as “Process C” in the IF-THEN-ELSE (Fig 4-2) to be recognized as completing the IF-THEN-ELSE rather than part of a higher level Sequence that included the IF-THEN-ELSE as a component.

Figures 1-6

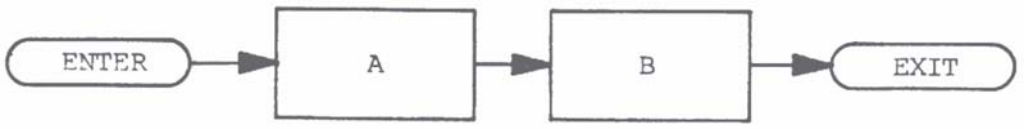

Figure 1 SEQUENCE

Control flows from “Process A” to the next in sequence, “Process B”

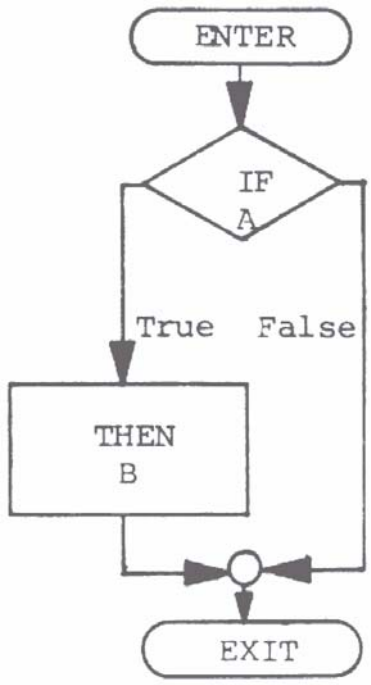

Figure 2 IF-THEN-ELSE

*****In Figure 2, flow of control will skip a process pending the condition of “A."

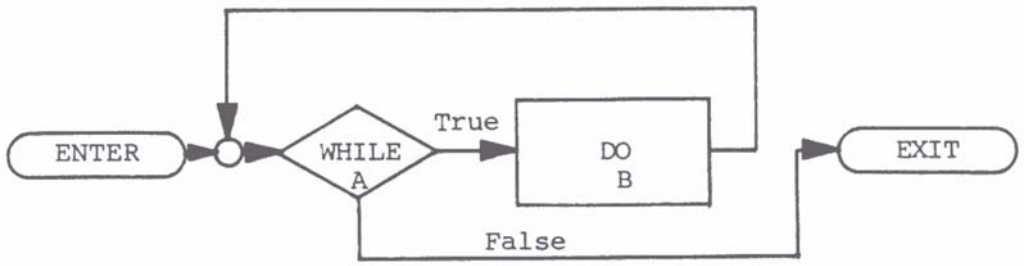

Figure 3 DO-WHILE

In Figure 4-3, condition “A” is evaluated. If found to be true, then control is passed to Process “B” and condition “A” is reevaluated. If condition “A” is found to be false, then control is passed out of the loop. Note that, if B is a BLOCK, the “DO” may be recognized as the opening symbol. A terminating symbol is needed from the language used.

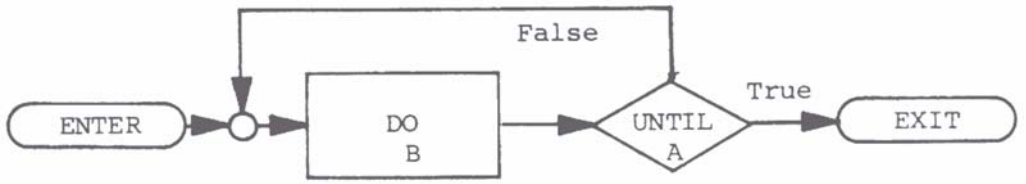

Figure 4 DO-UNTIL

Figure 4-4 is similar to a DO-WHILE, except that the test of condition A is performed after “Process B” has executed and the DO is performed upon a false “A” condition.. If condition “A” is true, control is passed out of the loop.

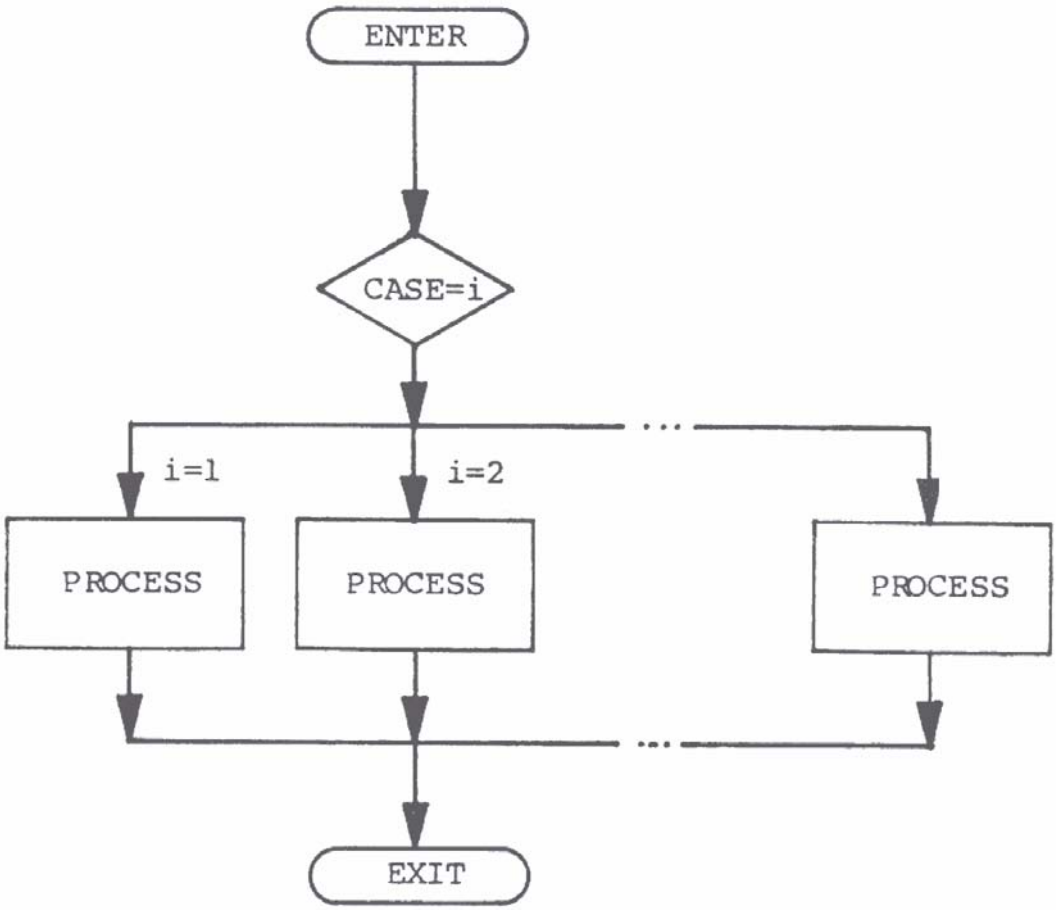

Figure 5 CASE

Control is passed to a Process based on the value of i.

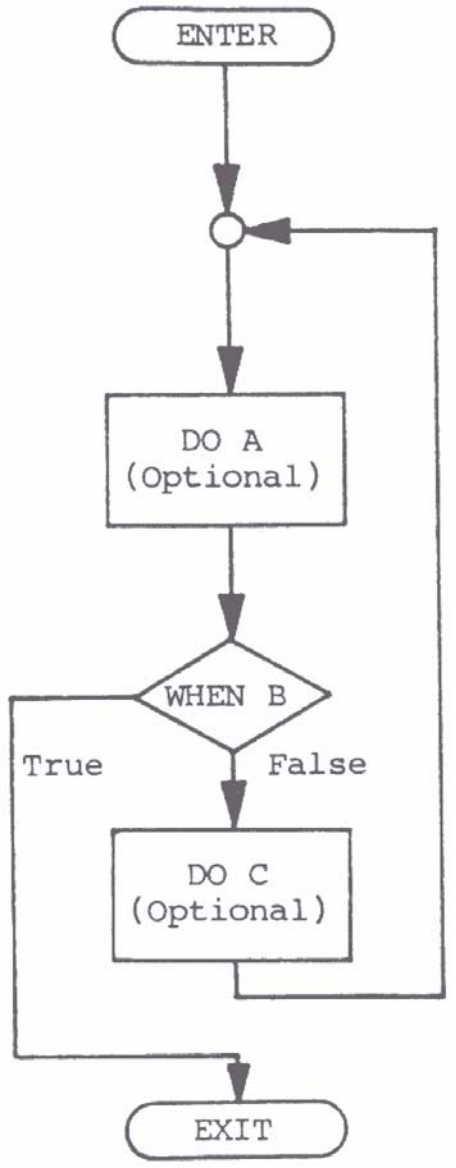

Figure 6 General LOOP

Optional process A is executed. Condition B is then evaluated. If found to be false, optional process C is executed and control is passed to process A. Condition B is then evaluated again. If condition B is true, then control is passed out of the loop.

A special case of the GENERAL LOOP is the FOR loop. The FOR loop is not strictly essential, as it can be programmed as a DO-WHILE loop. The FOR loop executes on a counter. The control FOR statement defines a counter variable or variables, a test for ending the loop, and a standard method of changing the variable(s) on each pass such as incrementing or decrementing. For example,

"FOR c = 0; c < 10; c + 1

DO Process A;"

The counter is initialized to zero, if the counter test is false, the DO process is executed and the counter is incremented (or decremented). Once the counter test is true, control exits from the loop without incrementing the counter. The implementation of the FOR loop in many languages, however, can be error prone. The use of the FOR loop shall include strictly enforced coding conventions to avoid common errors such as a loop that never ends.

The GENERAL LOOP should not be used where one of the other loop structures will serve. It is error prone and may not be supported in many languages without using GOTOs type redirections. However, if defined in the language, it may be useful in defining some loops where the exit needs to occur in the middle. Also, in other languages the GENERAL LOOP logic can be used to simulate the other control constructs. Like the special case, the use of the GENERAL LOOP shall require the strict enforcement of coding conventions to avoid problems.

5.4.2 Assessment of Coding Conventions

The accredited test lab shall test for compliance with the coding conventions specified by the vendor. If the vendor does not identify an appropriate set of coding conventions in accordance with the provisions of Volume I, Subsection 5.2.6, the accredited test lab shall review the code to ensure that it:

a. Uses uniform calling sequences. All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the type and range for the reference of the programmer and tester. Validation may be performed implicitly by the compiler or explicitly by the programmer

b. Has the return explicitly defined for callable units such as functions or procedures (do not drop through by default) for C-based languages and others to which this applies, and in the case of functions, has the return value explicitly assigned. Where the return is only expected to return a successful value, the C convention of returning zero shall be used or the use of another code justified in the comments. If an uncorrected error occurs so the unit must return without correctly completing its objective, a non-zero return value shall be given even if there is no expectation of testing the return. An exception may be made where the return value of the function has a data range including zero

c. Does not use macros that contain returns or pass control beyond the next statement

d. For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries

e. For those languages with pointers or which provide for specifying absolute memory locations, provides controls that prevent the pointer or address from being used to

overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored

f. For those languages supporting case statements, has a default choice explicitly defined to catch values not included in the case list

g. Provides controls to prevent any vote counter from overflowing. Assuming the counter size is large enough such that the value will never be reached is not adequate

h. Is indented consistently and clearly to indicate logical levels

i. Excluding code generated by commercial code generators, is written in small and easily identifiable modules, with no more than 50% of all modules exceeding 60 lines in length, no more than 5% of all modules exceeding 120 lines in length, and no modules exceeding 240 lines in length. "Lines" in this context, are defined as executable statements or flow control statements with suitable formatting and comments. The reviewer should consider the use of formatting, such as blocking into readable units, which supports the intent of this requirement where the module itself exceeds the limits. The vendor shall justify any module lengths exceeding this standard

j. Where code generators are used, the source file segments provided by the code generators should be marked as such with comments defining the logic invoked and, if possible, a copy of the source code provided to the accredited test lab with the generated source code replaced with an unexpanded macro call or its equivalent

k. Has no line of code exceeding 80 columns in width (including comments and tab expansions) without justification

l. Contains no more than one executable statement and no more than one flow control statement for each line of source code

m. In languages where embedded executable statements are permitted in conditional expressions, the single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to other lines

n. Avoids mixed-mode operations. If mixed mode usage is necessary, then all uses shall be identified and clearly explained by comments

o. Upon exit() at any point, presents a message to the user indicating the reason for the exit()

p. Uses separate and consistent formats to distinguish between normal status and error or exception messages. All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician

q. References variables by fewer than five levels of indirection (i.e., a.b.c.d or a[b].c->d)

r. Has functions with fewer than six levels of indented scope, counted as follows:

```
int function()
{
        if (a = true)
1       {
                if ( b = true )
2               {
                                        if ( c = true )
3                       {
                                                if ( d = true )
4                               {
                                        while(e > 0 )
5                                       {
                                                                code
                                                                }
                                                }
                                        }
                               }
                       }
                       }
```

s. Initializes every variable upon declaration where permitted

t. Has all constants other than 0 and 1 defined or enumerated, or shall have a comment which clearly explains what each constant means in the context of its use. Where "0" and "1" have multiple meanings in the code unit, even they should be identified. Example: "0" may be used as FALSE, initializing a counter to zero, or as a special flag in a non-binary category

u. Only contains the minimum implementation of the "a = b ? c : d" syntax. Expansions such as "j=a?(b?c:d):e;" are prohibited

v. Has all assert() statements coded such that they are absent from a production compilation. Such coding may be implemented by ifdef()s that remove them from or include them in the compilation. If implemented, the initial program identification in setup should identify that assert() is enabled and active as a test version

6 System Integration Testing

Table of Contents

6 System Integration Testing

6.1 Scope

This section contains a description of the testing to be performed by the accredited test lab to confirm the proper functioning of the fully integrated components of a voting system submitted for national certification testing. It describes the scope and basis for integration testing, testing of internal and external system interfaces, testing of security capabilities, and the configuration audits, including the testing of system documentation.

System level certification tests address the integrated operation of both hardware and software, along with any telecommunications capabilities. The system level certification tests shall include the tests (functionality, volume, stress, usability, security, performance, and recovery) indicated in the National Certification Test Plan, described in Appendix A. These tests assess the system's response to a range of both normal and abnormal conditions initiated in an attempt to compromise the system. These tests may be part of the audit of the system's functional attributes, or may be conducted separately.

The system integration tests include two audits: a Physical Configuration Audit that focuses on physical attributes of the system, and a Functional Configuration Audit that focuses on the system's functional attributes, including attributes that go beyond the specific requirements of the Standards.

6.2 Basis of Integration Testing

This subsection addresses the basis for integration testing, the system baseline for testing, and data volumes for testing.

6.2.1 Testing Breadth

The accredited test lab shall design and perform procedures that test the voting system capabilities for the system as a whole. These procedures follow the testing of the systems hardware and software, and address voting system requirements defined in Volume I, Sections 2, 4, 5 and 6.

These procedures shall also address the requirements for testing system functionality provided in Section 3. Where practical, the accredited test lab will perform coverage reporting of the software branches executed in the functional testing. The selection of the baseline test cases will follow an operational profile of the common procedures, sequencing, and options among the shared state requirements and those that are specifically recognized and supported by the vendor. The accredited test lab will use the coverage report to identify any portions of the source code that were not covered and determine:

a. The additional functional tests that are needed

b. Where more detailed source code review is needed

c. Both of the above

The specific procedures to be used shall be identified in the National Certification Test Plan. These procedures may replicate testing performed by the vendor and documented in the vendor's TDP, but shall not rely on vendor testing as a substitute for testing performed by the accredited test lab.

Recognizing variations in system design and the technologies employed by different vendors, the accredited test lab shall design test procedures that account for these variations.

6.2.2 System Baseline for Testing

The system level certification tests are conducted using the version of the system intended to be sold by the vendor and delivered to jurisdictions. To ensure that the system version tested is the correct version, the accredited test lab shall witness the build of the executable version of the system immediately prior to or as part of, the physical configuration audit. Additionally, should components of the system be modified or replaced during the testing process, the accredited test lab shall require the vendor to conduct a new "build" of the system to ensure that the certified executable release of the system is built from tested components.

6.2.3 Testing Volume

For all systems, the total number of ballots to be processed by each precinct counting device during these tests shall reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support.

6.3 Testing Interfaces of System Components

The accredited test lab shall design and perform test procedures that test the interfaces of all system modules and subsystems with each other against the vendor's specifications. These tests shall be documented in the National Certification Test Plan, and shall include the full range of system functionality provided by the vendor's specifications, including functionality that exceeds the specific requirements of these Guidelines.

Some voting systems may use components or subsystems from previously tested and qualified systems, such as ballot preparation. For these scenarios, the accredited test lab shall, at a minimum:

a. Confirm that the version of previously approved components and subsystems is unchanged

b. Test all interfaces between previously approved modules/subsystems and all other system modules and subsystems. Where a component is expected to interface with several different products, especially from different manufacturers, the vendor shall provide a public data specification of files or data objects used to exchange information

Some systems use telecommunications capabilities. For those systems that do use such capabilities, components that are located at the polling place or separate vote counting location shall be tested for effective interface, accurate vote transmission, failure detection, and failure recovery. For voting systems that use telecommunications lines or networks that are not under the control of the election official (e.g., public telephone networks), the accredited test lab shall test the interface of vendor-supplied components with these external components for effective interface, vote transmission, failure detection, and failure recovery.

6.4 Security Testing

The accredited test lab shall design and perform test procedures that test the security capabilities of the voting system against the requirements defined in Volume I, Section 7. These procedures shall focus on the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the vendor in the TDP to go beyond these risks. The range of risks tested is determined by the design of the system and potential exposure to risk. Regardless of system design and risk profile, all systems shall be tested for effective access control and physical data security.

For systems that use public telecommunications networks, including the Internet, to transmit election management data or official election results (such as ballots or tabulated results), the accredited test lab shall conduct tests to ensure that the system provides the necessary identity-proofing, confidentiality, and integrity of transmitted data. These tests shall be designed to confirm that the system is capable of detecting, logging, preventing, and recovering from types of attacks known at the time the system is submitted for certification.

The accredited test lab may meet these testing requirements by confirming proper implementation of proven commercial security software. In this case, the vendor must provide the published standards and methods used by the U.S. Government to test and accept this software, or it may provide references to free, publicly available publications of these standards and methods, such as government web sites.

At its discretion, the accredited test lab may conduct or simulate attacks on the system to confirm the effectiveness of the system's security capabilities, employing test procedures approved by the EAC.

6.4.1 Access Control

The accredited testing laboratory shall conduct tests of system capabilities and review the access control policies and procedures submitted by the vendor to identify and verify the access control features implemented as a function of the system. For those access control features built in as components of the voting system, the accredited test lab shall design tests to confirm that these security elements work as specified.

Specific activities to be conducted by the accredited test lab shall include:

a. A review of the vendor's access control policies, procedures and system capabilities to confirm that all requirements of Volume I, Subsection 7.2 have been addressed completely

b. Specific tests designed by the accredited test lab to verify the correct operation of all documented access control procedures and capabilities, including tests designed to circumvent controls provided by the vendor. These tests shall include:

    i. Performing the activities that the jurisdiction will perform in specific accordance with the vendor's access control policy and procedures to create a secure system, including procedures for software and firmware installation (as described in Volume I, Subsection 7.4)

    ii. Performing tests intended to bypass or otherwise defeat the resulting security environment. These tests shall include simulation of attempts to physically destroy components of the voting system in order to validate the correct operation of system redundancy and backup capabilities

This review applies to the full scope of system functionality. It includes functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote canvassing, vote reporting, and maintenance of the system's audit trail.

6.4.2 Data Interception and Disruption

For systems that use telecommunications to transmit official voting data, the accredited test lab shall review, and conduct tests of, the data interception and prevention safeguards specified by the vendor in its TDP. The accredited test lab shall evaluate safeguards provided by the vendor to ensure their proper operation, including the proper response to the detection of efforts to monitor data or otherwise compromise the system.

For systems that use public communications networks the accredited test lab shall also review the vendor's documented procedures for maintaining protection against newly discovered external threats to the telecommunications network. This review shall assess the adequacy of such procedures in terms of:

a. Identification of new threats and their impact

b. Development or acquisition of effective countermeasures

c. System testing to ensure the effectiveness of the countermeasures

d. Notification of client jurisdictions that use the system of the threat and the actions that should be taken

e. Distribution of new system releases or updates to current system users

f. Confirmation of proper installation of new system releases

6.5 Usability and Accessibility Testing

The vendor shall design and perform procedures that test the usability and accessibility of the voting system as defined in Volume I, Section 3. Test procedures shall confirm that:

a. All voting machines meet the usability requirements specified in Volume I, Subsection 3.1

b. Voting machines intended for use by voters with disabilities provide the capabilities required by Volume I, Subsection 3.2

c. Voting machines intended for use by voters with disabilities operate consistently with vendor specifications and documentation

6.6 Physical Configuration Audit

The Physical Configuration Audit compares the voting system components submitted for qualification to the vendor's technical documentation, and shall include the following activities:

a. The audit shall establish a configuration baseline of the software and hardware to be tested. It shall also confirm whether the vendor's documentation is sufficient for the user to install, validate, operate, and maintain the voting system. MIL-STD-1521 can be used as a guide when conducting this audit

b. The test agency shall examine the vendor's source code against the submitted documentation during the Physical Configuration Audit to verify that the software conforms to the vendor's specifications. This review shall include an inspection of all records of the vendor's release control system. If changes have been made to the baseline version, the accredited test lab shall verify that the vendor's engineering and test data are for the software version submitted for certification

c. If the software is to be run on any equipment other than a COTS mainframe data processing system, minicomputer, or microcomputer, the Physical Configuration Audit shall also include a review of all drawings, specifications, technical data, and

test data associated with the system hardware. This examination shall establish the system hardware baseline associated with the software baseline

d. To assess the adequacy of user acceptance test procedures and data, vendor documents containing this information shall be reviewed against the system's functional specifications. Any discrepancy or inadequacy in the vendor's plan or data shall be resolved prior to beginning the system integration functional and performance tests

e. All subsequent changes to the baseline software configuration made during the course of testing shall be subject to re-examination. All changes to the system hardware that may produce a change in software operation shall also be subject to re-examination

The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor technical personnel shall be available to assist in the performance of the Physical Configuration Audit.

6.7 Functional Configuration Audit

The Functional Configuration Audit encompasses an examination of vendor tests, and the conduct of additional tests, to verify that the system hardware and software perform all the functions described in the vendor's documentation submitted for the TDP. It includes a test of system operations in the sequence in which they would normally be performed, and shall include the following activities. MIL-STD-1521 may be used as a guide when conducting this audit:

a. The accredited test lab shall review the vendor's test procedures and test results to determine if the vendor's specified functional requirements have been adequately tested. This examination shall include an assessment of the adequacy of the vendor's test cases and input data to exercise all system functions, and to detect program logic and data processing errors, if such be present

b. The accredited test lab shall perform or supervise the performance of additional tests to verify nominal system performance in all operating modes, and to verify on a sampling basis the vendor's test data reports. If vendor developmental test data is incomplete, the accredited test lab shall design and conduct all appropriate module and integrated functional tests. The functional configuration audit may be performed in the facility either of the accredited test lab or of the vendor, and shall use and verify the accuracy and completeness of the System Operations, Maintenance, and Diagnostic Testing Manuals

The vendor shall provide a list of all documentation and data to be audited, cross-referenced to the contents of the TDP. Vendor technical personnel shall be available to assist in the performance of the Functional Configuration Audit.

7 Quality Assurance Testing

Table of Contents

7 Quality Assurance Testing

7.1 Scope

This section contains a description of the examination performed by the accredited test lab to verify conformance with the requirements for configuration management and quality assurance of voting systems. It describes the scope and basis for the examinations, the general sequence of the examinations within the overall test process, and provides guidance on the substantive focus of the examinations.

7.2 Basis of Examinations

The accredited test lab shall design and perform procedures that examine documented vendor practices for quality assurance and configuration management as addressed by Volume I, Sections 8 and 9 and Section 2.
Examination procedures shall be designed and performed to ensure:

a. Conformance with the requirements to provide information on vendor practices required by these *Guidelines*

b. Conformance of system documentation and other information provided by the vendor with the documented practices for quality assurance and configuration management

The *Guidelines* do not require on-site examination of the vendor's quality assurance and configuration management practices during the system development process. However, the accredited test lab can conduct several activities while at the vendor site to witness the system build that enable assessment of the vendor's quality assurance and configuration management practices. These include surveys, interviews with individuals at all levels of the development team, and examination of selected internal work products such as system change requests and problem tracking logs.

It is recognized that examinations of vendor practices, and determinations of conformance, entail a significant degree of professional judgment. These guidelines for vendor practices identify specific areas of focus but heavily rely on the expertise and professional judgment, of the accredited test lab.

The specific procedures used by the accredited test lab shall be identified in the Qualification Test Plan. Recognizing variations in vendors' quality assurance and configuration management practices and procedures, the accredited test lab shall design examination procedures that account for these variations.

7.3 General Examinations Sequence

There is no required sequence for performing the examinations of quality assurance and configuration management practices. No other testing is dependent on the performance and results of these examinations. However, examinations pertaining to configuration management, in particular those pertaining to configuration identification, will generally be useful in understanding the conventions used to define and document the components of the system and will assist with other elements of the certification test process.

7.3.1 Vendor Practices in Parallel with Other Certification Testing

While not required, the accredited test lab is encouraged to initiate the examinations of quality assurance and configuration management practices early in the overall testing sequence, and to conduct them in parallel with other testing of the voting system. Conducting these examinations in parallel is recommended to minimize the overall duration of the testing process.

7.3.2 Functional Configuration Audit and System Integration Testing

As described in Volume I, Section 9, the functional configuration audit verifies that the voting system performs all the functions described in the system documentation. To help ensure an efficient test process, this audit shall be conducted by the accredited test lab as an element of the system integration testing that confirms the proper functioning of the system as a whole.

7.4 Examination of Configuration Management Practices

The examination of configuration management practices shall address the full scope of requirements described in Volume I, Section 9, and the documentation requirements described in Section 2. In addition to confirming that all required information has been submitted, the accredited test lab shall determine the vendor's conformance with the documented configuration management practices.

7.4.1 Configuration Management Policy

The accredited test lab shall examine the vendor's documented configuration management policy to confirm that it:

a. Addresses the full scope of the system, including components provided by external suppliers

b. Addresses the full breadth of system documentation

7.4.2 Configuration Identification

The accredited test lab shall examine the vendor's documented configuration identification practices policy to confirm that it:

a. Describes clearly the basis for classifying configuration items into categories and subcategories, for numbering of configuration items; and for naming of configuration items

b. Describes clearly the conventions used to identify the version of the system as a whole and the versions of any lower level elements (e.g., subsystems, individual elements) if such lower level version designations are used

7.4.3 Baseline, Promotion, and Demotion Procedures

The accredited test lab shall examine the vendor's documented baseline, promotion, and demotion procedures to confirm that they:

a. Provide a clear, controlled process that promotes components to baseline status when specific criteria defined by the vendor are met; and

b. Provide a clear, controlled process for demoting a component from baseline status when specific criteria defined by the vendor are met.

7.4.4 Configuration Control Procedures

The accredited test lab shall examine the vendor's configuration control procedures to confirm that they:

a. Are capable of providing effective control of internally developed system components

b. Are capable of providing effective control of components developed or supplied by third parties

7.4.5 Release Process

The accredited test lab shall examine the vendor's release process to confirm that it:

a. Provides clear accountability for moving forward with the release of the initial system version and subsequent releases

b. Provides the means for clear identification of the system version being replaced

c. Confirms that all required internal vendor tests and audits prior to release have been completed successfully

d. Confirms that each system version released to customers has been certified

e. Confirms that each system release has been received by the customer

f. Confirms that each system release has been installed successfully by the customer

7.4.6 Configuration Audits

The accredited test lab shall examine the vendor's configuration audit procedures to confirm that they:

a. Are sufficiently broad in scope to address the entire system, including system documentation

b. Are conducted with appropriate timing to enable effective control of system versions

c. Are sufficiently rigorous to confirm that all system documentation prepared and maintained by the vendor matches the actual system functionality, design, operation, and maintenance requirements

7.4.7 Configuration Management Resources

The accredited test lab shall examine the configuration management resource information submitted by the vendor to determine whether sufficient information has been provided to enable another organization to clearly identify the resources used and acquire them for use. This examination is intended to ensure that in the event the vendor concludes business operations, sufficient information has been provided to enable an in-depth audit of the system should such an audit be required by election officials and/or a law enforcement organization.

7.5 Examination of Quality Assurance Practices

The examination of quality assurance practices shall address the full scope of requirements described in Volume I, Section 8, and the documentation requirements described in Volume II, Section 2. The accredited test lab shall confirm that all required information has been submitted, and assess whether the vendor's quality assurance program provides for:

a. Clearly measurable quality standards

b. An effective testing program throughout the system development life cycle

c. Application of the quality assurance program to external providers of system components and supplies

d. Comprehensive monitoring of system performance in the field and diagnosis of system failures

e. Effective record keeping of system failures to support analysis of failure patterns and potential causes

f. Effective processes for notifying customers of system failures and corrective measures that need to be taken, and for confirming that such measures are taken

In addition to the general examinations described above, the accredited test lab shall focus on the specific elements of the vendor's quality assurance program indicated below.

7.5.1 Quality Assurance Policy

The accredited test lab shall examine the vendor's quality assurance policy to confirm that it:

a. Addresses the full scope of the voting system

b. Clearly designates a senior level individual accountable for implementation and oversight of quality assurance activities

c. Clearly designates the individuals, by position within the vendor's organization, who are to conduct each quality assurance activity

d. Provides procedures that determine compliance with, and correct deviations from, the quality assurance program at a minimum annually

7.5.2 Parts and Materials Tests

The accredited test lab shall examine the vendor's parts and materials special tests and examinations to confirm that they:

a. Identify appropriate criteria that are used to determine the specific system components for which special tests are required to confirm their suitability for use in a voting system

b. Are designed in a manner appropriate to determine suitability

c. Have been conducted and documented for all applicable parts and materials

7.5.3 Quality Conformance Inspections

The accredited test lab shall examine the vendor's quality conformance plans, procedures and, inspection results to confirm that:

a. All components have been tested according to the test requirements defined by the vendor

b. All components have passed the requisite tests

c. For each test, the test documentation identifies:

   i. Test location

   ii. Test date

   iii. Individual who conducted the test

   iv. Test outcome

7.5.4 Documentation

The accredited test lab shall examine the vendor's voting system documentation to confirm that it meets the content requirements of Volume I, Subsection 8.7, and Section 2, and is written in a manner suitable for use by purchasing jurisdictions.

Appendix A: National Certification Test Plan

Table of Contents

Appendix A: National Certification Test Plan

A.1 Scope

This Appendix contains a recommended outline for the National Certification Test Plan, which is to be prepared by the test lab. The primary purpose of the test plan is to document the test lab's development of the complete or partial certification test. A sample outline is provided in Figure A-1 at the end of this Appendix.

It is intended that the test lab use this Appendix as a guide in preparing a detailed test plan, and that the scope and detail of the requirements for certification be tailored to the type of hardware, and the design and complexity of the software being tested. Required hardware tests are defined in Section 4, whereas software and system-level tests must be developed based on the vendor pre-certification tests and information available on the specific software's physical and functional configuration.

Prior to development of any test plan, the test lab must obtain the Technical Data Package (TDP) from the vendor submitting the voting system for certification. The TDP contains information necessary to the development of the test plan, such as the vendor's Hardware Specifications, Software Specifications, System Operating Manual and System Maintenance Manual.

It is specified by the *Guidelines* that voting systems incorporating the vendor's software and COTS hardware need only be submitted for software and system level tests. Recertification of systems with modified software or hardware is also anticipated. The test lab shall alter the test plan outline as required by these situations.

The following discussion describes the individual sections of the recommended National Certification Test Plan. The test lab shall include the identification, and a brief description of, the hardware and software to be tested, and any special considerations that affect the test design and procedure.

A.1.1 References

The test lab shall list all documents that contain material used in preparing the test plan. This list shall include specific references to applicable portions of the guidelines, and to the vendor’s TDP.

A.1.2 Terms and Abbreviations

The test lab shall list and define all terms and phrases relevant to the hardware, the software, or the test plan.

A.2 Pre-certification Tests

The test lab shall evaluate vendor tests, or other lab tests in determining the scope of testing required for system certification. Pre-certification test activities may be particularly useful in designing software functional test cases and tests of system security. The test lab shall summarize pre-certification test results that support the discussion of the preceding section.

A.3 Materials Required for Testing

The following materials must be provided to the test lab to facilitate testing of the voting system:

a. Software

b. Equipment

c. Test materials

d. Deliverable materials

e. Proprietary data

A.3.1 Software

The test lab shall list all software required for the performance of hardware, software, telecommunications, security and system integration tests. If the test environment requires supporting software such as operating systems, compilers, assemblers, or database managers, then this software shall also be listed.

A.3.2 Equipment

The test lab shall list all equipment required for the performance of the hardware, software, telecommunications, security and system integration tests. This list shall include system hardware, general purpose data processing and communications equipment, and test instrumentation, as required.

A.3.3 Test Materials

The test lab shall list all test materials required in the performance of the test including, as applicable, test ballot layout and generation materials, test ballot sheets, test ballot cards and control cards, standard and optional output data report formats, and any other materials used to simulate preparation for, and conduct of, elections.

A.3.4 Deliverable Materials

The test lab shall list all documents and materials to be delivered as a part of the system, such as:

a. Hardware specification

b. Software specification

c. Voter, operator, hardware, and software maintenance manuals

d. Program listings, facsimile ballots, tapes

e. Sample output report formats

A.3.5 Proprietary Data

The test lab shall list and describe all documentation and data that are proprietary to the vendor, and hence are subject to restrictions with respect to test lab use, release, or disclosure.

A.4 Test Specifications

The test lab shall cite the pertinent hardware qualitative examinations and quantitative tests that follow from Volume I, Sections 2, 4, 5, 6, 7 and 8. The test lab shall also describe the specific test requirements that follow from the design of the software and telecommunications capabilities under test.

The certification test shall include hardware, software and telecommunications design and the development and conduct of all tests to demonstrate satisfactory performance. Environmental, non-operating tests shall be performed in the categories of simulated environmental conditions specified by the vendor or user requesting the tests. Environmental operating tests shall be performed under varying temperatures. Other functional tests shall be conducted in an environment that simulates, as nearly as possible, the intended use environment.

Test hardware and software shall be identical to that designed to be used together in the voting system, except that software intended for use with general purpose off-the-shelf hardware may be tested using any equivalent equipment capable of supporting its operation and functions.

A.4.1 Hardware Configuration and Design

The test lab shall document the hardware configuration and design in detail sufficient to identify the specific equipment being tested. This document shall provide a basis for the specific test design and include a brief description of the intended use of the hardware.

A.4.2 Software System Functions

The test lab shall describe the software functions in sufficient detail to provide a foundation for selecting the test case designs and conditions described in Section A.4.3. On the basis of this test case design, the test lab shall prepare a table delineating software functions and how each shall be tested.

A.4.3 Test Case Design

The test lab shall examine the test case design of the following aspects of the voting system:

a. Hardware qualitative examination design

b. Hardware environmental test case design

c. Software module test case design and data

d. Software functional test case design

e. System level test case design

A.4.3.1 Hardware Qualitative Examination Design

The test lab shall review the results, submitted by the vendor, of any previous examinations of the equipment to be tested. The results of these examinations shall be compared to the performance characteristics specified by Section 2 of the *Guidelines* concerning the requirements for:

a. Overall system capabilities

b. Pre-voting functions

c. Voting functions

d. Post-voting functions

In the event that a review of the results of previous examinations indicates problem areas, the test lab shall provide a description of further examinations required prior to conducting the environmental and system level tests. If no previous examinations have been performed, or records of these tests are not available, the test agency shall specify the appropriate tests to be used in the examination.

A.4.3.2 Hardware Environmental Test Case Design

The test lab shall review the documentation, submitted by the vendor, of the results and design of any previous environmental tests of the equipment submitted for testing. The test design and results shall be compared to the tests described in Section 1. The test lab shall cite any additional tests required, based on this review and those tests requested by the vendor or the state. The test lab shall also cite any environmental tests that are not to be conducted, and note the reasons why.

For complete certification, environmental tests shall include the following tests, depending upon the design and intended use of the hardware:

a. Non-operating tests, including the:

   i. Bench handling test

   ii. Vibration test

   iii. Low temperature test

   iv. High temperature test

   v. Humidity test

b. Operating tests involving a series of procedures that test system reliability and accuracy under various temperatures and voltages relevant to election use

A.4.3.3 Software Module Test Case Design and Data

The test lab shall review the vendor's program analysis, documentation, and, if available, module test case design. The test lab shall evaluate the test cases for each module, with respect to flow control parameters and data on both entry and exit. All discrepancies between the Software Specifications and the test case design shall be corrected by the vendor prior to initiation of the certification test.

If the vendor's module test case design does not provide conclusive coverage of all program paths, then the test lab shall perform an independent analysis to assess the frequency and consequence of error of the untested paths. The test lab shall design additional module test cases, as required, to provide coverage of all modules containing untested paths with potential for untrapped errors.

The test lab shall also review the vendor's module test data in order to verify that the requirements of the Software Specifications have been demonstrated by the data. In the event that the vendor's module test data are insufficient, the test lab shall provide a description of additional module tests, prerequisite to the initiation of functional tests.

A.4.3.4 Software Functional Test Case Design

The test lab shall review the vendor's test plans and data to verify that the individual performance requirements described in Subsection 2.5.3, are reflected in the software.

As a part of this process, the test lab shall review the vendor's functional test case designs. The test lab shall prepare a detailed matrix of system functions and the test cases that exercise them. The test lab shall also prepare a test procedure describing all test ballots, operator procedures, and the data content of output reports. Abnormal input data and operator actions shall be defined. Test cases shall also be designed to verify that the system is able to handle and recover from these abnormal conditions.

The vendor's test case design may be evaluated by any standard or special method appropriate; however, emphasis shall be placed on those functions where the vendor data on module development reflects significant debugging problems, and on functional tests that resulted in disproportionately high error rates.

The test lab shall define ACCEPT/REJECT criteria for certification using the Software Specifications and, if the software runs on special hardware, the associated Hardware Specifications to determine acceptable ranges of performance.

The test lab shall describe the functional tests to be performed. Depending upon the design and intended use of the voting system, all or part of the functions listed below shall be tested.

a. Ballot preparation subsystem

b. Test operations performed prior to, during, and after processing of ballots, including:

    i. Logic tests to verify interpretation of ballot styles, and recognition of precincts to be processed

    ii. Accuracy tests to verify ballot reading accuracy

    iii. Status tests to verify equipment statement and memory contents

iv. Report generation to produce test output data

v. Report generation to produce audit data records

c. Procedures applicable to equipment used in the polling place for:

i. Opening the polling place and enabling the acceptance of ballots and maintaining a count of processed ballots

ii. Monitoring equipment status

iii. Verifying equipment response to operator input commands

iv. Generating real-time audit messages

v. Closing the polling place and disabling the acceptance of ballots

vi. Generating election data reports

vii. Transfer of ballot counting equipment, or a detachable memory module, to a central counting location

viii. Electronic transmission of election data to a central counting location

d. Procedures applicable to equipment used in a central counting place:

i. Initiating the processing of a ballot deck or programmable memory device for one or more precincts

ii. Monitoring equipment status

iii. Verifying equipment response to operator input commands

iv. Verifying interaction with peripheral equipment, or other data processing systems

v. Generating real-time audit messages

vi. Generating precinct-level election data reports

vii. Generating summary election data reports

viii. Transfer of a detachable memory module to other processing equipment

ix. Electronic transmission of data to other processing equipment

x. Producing output data for interrogation by external display devices

A.4.3.5 System-level Test Case Design

The test lab shall provide a description of system tests of both the software and hardware. For software, these tests shall be designed according to the stated design objective without consideration of its functional specification. The test lab shall independently prepare the system test cases to assess the response of the hardware and software to a range of conditions, such as:

a. **Volume tests:** These tests investigate the system's response to processing more than the expected number of ballots/voters per precinct, to processing more than the expected number of precincts, or to any other similar conditions that tend to overload the system's capacity to process, store, and report data.

b. **Stress tests:** These tests investigate the system's response to transient overload conditions. Polling place devices shall be subjected to ballot processing at the high volume rates at which the equipment can be operated to evaluate software response to hardware-generated interrupts and wait states. Central counting systems shall be subjected to similar overloads, including, for systems that support more than one card reader, continuous processing through all readers simultaneously.

c. **Usability tests:** These tests are designed to exercise characteristics of the software such as response to input control or text syntax errors, error message content, audit message content, and other features contained in the software design objectives but not directly related to a functional specification.

d. **Accessibility tests:** The test lab shall review the vendor’s documentation of the usability and accessibility testing performed during system development.

e. **Security tests:** These tests are designed to defeat the security provisions of the system including modification or disruption of pre-voting, voting, and post voting processing; unauthorized access to, deletion, or modification of data, including audit trail data; and modification or elimination of security mechanisms.

f. **Performance tests:** These tests verify accuracy, processing rate, ballot format handling capability, and other performance attributes claimed by the vendor.

g. **Recovery tests:** These tests verify the ability of the system to recover from hardware and data errors.

A.5 Test Data

A.5.1 Data Recording

The test lab shall identify all data recording requirements (e.g.; what is to be measured, how tests and results are to be recorded). The test lab shall also design or approve the design of

forms or other recording media to be employed. The test lab shall supply any special instrumentation (e.g., pulse measuring device) needed to satisfy the data requirements.

A.5.2 Test Data Criteria

The test lab shall describe the criteria against which test results will be evaluated, such as the following:

a. **Tolerances:** These criteria define the acceptable range for system performance. These tolerances shall be derived from the applicable hardware performance requirements contained in Volume I, Section 4

b. **Samples:** These criteria define the minimum number of combinations or alternatives of input and output conditions that can be exercised to constitute an acceptable test of the parameters involved

c. **Events:** These criteria define the maximum number of interrupts, halts or other system breaks that may occur due to nontest conditions. This count shall not include events from which recovery occurs automatically or where a relevant status message is displayed

A.5.3 Test Data Reduction

The test lab shall describe the techniques to be used for processing test data. These techniques may include manual, semi-automatic, or fully automatic reduction procedures. However, semi-automatic and automatic procedures must be demonstrated to be capable of handling the test data accurately and properly. They shall also produce an item-by-item comparison of the data and the embedded acceptance criteria as output.

A.6 Test Procedure and Conditions

The test lab shall describe the test conditions and procedures for performing the tests. If tests are not to be performed in random order, this section shall contain the rationale for the required sequence, and the criteria that must be met, before the sequence can be continued. This section shall also describe the procedure for setting up the equipment in which the software will be tested, for system initialization, and for performing the tests. Each of the following sections that contain a description of a test procedure shall also contain a statement of the criteria by which readiness and successful completion shall be indicated and measured.

A.6.1 Facility Requirements

The test lab shall describe the space, equipment, instrumentation, utilities, manpower, and other resources required to support the test program.

A.6.2 Test Set-up

The test lab shall describe the procedure for arranging and connecting the system hardware with the supporting hardware and telecommunications equipment, if applicable. It shall also describe the procedure required to initialize the system, and to verify that it is ready to be tested.

A.6.3 Test Sequence

The test lab shall state any restrictions on the grouping or sequence of tests in this section.

A.6.4 Test Operations Procedures

The test lab shall provide the step-by-step procedures for each test case to be conducted. Each step shall be assigned a test step number and this number, along with critical test data and test procedures information, shall be tabulated onto a test report form for test control and the recording of test results.

In this section, the test lab shall also identify all test operations personnel, and their respective duties. In the event that the operator procedure is not defined in the vendor's operations or user manual, the test lab shall also provide a description of the procedures to be followed by the test personnel.

Figure 1 Test Plan Outline

1 Introduction
1.1 References
1.2 Terms and Abbreviations

2 Pre-certification Tests
2.1 Pre-certification Test Activity
2.2 Pre-certification Test Results

3 Materials Required for Testing
3.1 Software
3.2 Equipment
3.3 Test Materials
3.4 Deliverable Materials
3.5 Proprietary Data

4 Test Specification
4.1 Requirements
4.2 Hardware Configuration and Design
4.3 Software System Functions
4.4 Test Case Design
4.4.1 Hardware Qualitative Examination Design
4.4.2 Hardware Environmental Test Case Design
4.4.3 Software Module Test Case Design and Data
4.4.4 Software Functional Test Case Design and Data
4.4.5 System-level Test Case Design

5 Test Data
5.1 Data Recording
5.2 Test Data Criteria
5.3 Test Data Reduction

6 Test Procedure and Conditions
6.1 Facility Requirements
6.2 Test Set-up
6.3 Test Sequence
6.4 Test Operations Procedures

Appendix B: National Certification Test Report

Table of Contents

Appendix B: National Certification Test Report

B.1 Scope

This Appendix contains a recommended outline for the National Certification Test Report to be prepared by the accredited test lab. The test report shall be organized so as to facilitate the presentation of conclusions and recommendations regarding system acceptability, a summary of the test operations, a summary of the test results, the test data records, and the analyses that support the conclusions and recommendations. The content of the report may vary based on the scope of review conducted.

B.1.1 New Certification Test Report

A full report is prepared for the initial certification testing of a voting system. This document consists of five main sections: Introduction, Certification Test Background, System Identification, System Overview, and Certification Test Results.

Detailed information about the test operations and findings, and test data, are included as appendices to the report.

Sections B.2 through B.7 describe the contents of the individual sections of this report.

B.1.2 Changes to Previously Certified Test Report

This report addresses a wide range of scenarios. After a preliminary review of the submitted changes, the accredited test lab may determine that:

a. A review of all change documentation against the baseline materials is sufficient for recommendation for certification

b. All changes must be retested against the previously certified baseline

c. The scope of the changes is substantial enough that a complete retest of the software is required

The format of this report will vary, based on the type of review that is performed. If only a review of change documentation against the baseline materials is performed the report is quite simple. It consists of an Introduction, a Version Description, the Testing Approach, and a Results Summary. A more extensive report is prepared, for changes that have extensive impact on the system design and/or operations.

B.2 Certification Test Background

This section contains the following information:

a. General information about the certification test process

b. A list and definition of all terms and nomenclature peculiar to the hardware, the software, or the test report

B.3 System Identification

This section gives information about the tested software and supporting hardware, including:

a. System name and major subsystems (or equivalent)

b. System version

c. Test support hardware

d. Specific documentation provided in the vendor's TDP used to support testing

B.4 System Overview

This section describes the voting system in terms of its overall design structure, technologies used, processing capacity claimed by the vendor for system components (such as ballot counters, voting machines, vote consolidation equipment), and mode of operation. It may also identify other products that interface with the voting system.

B.5 Certification Test Results and Recommendation

This section provides a summary of the results of the testing process, and indicates any special considerations that affect the conclusions derived from the test results. This summary includes:

a. The acceptability of the system design and construction based on the performance of the system hardware, software and communications, and on the source code inspection

b. The degree to which the hardware and software meet the vendor's specifications and the guidelines, and the acceptability of the vendor's technical and user documentation

c. General findings on the maintainability of the system including, where applicable, notation of specific maintenance activities that are determined to be difficult to perform

d. Identification and description of any deficiencies that remain uncorrected after completion of the certification test and that have caused or are judged to be capable of causing, the loss or corruption of voting data, providing sufficient detail to support a recommendation to reject the system being tested. Similarly, any deficiency in compliance with the security, accuracy, data retention, and audit requirements are fully described

e. A specific recommendation to the EAC for approval or rejection

Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I or failure to fully implement formal programs for quality assurance and configuration management described in Volume I, Sections 8 and 9. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system. The recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use.

B.6 Appendix – Test Operations and Findings

This appendix provides additional detail about the test results to enable the understanding of test results and recommendation. This information is organized in a manner that reflects the Certification Test Plan. Summaries of the results of hardware examinations, operating and non-operating hardware tests, software module tests, software function tests, and system-level tests (including security and telecommunications tests, and the results of the Physical and Functional Configuration Audits) are provided.

B.7 Appendix - Test Data Analysis

This appendix provides summary records of the test data and the details of the analysis. The analysis includes a comparison of the vendor's hardware and software specifications to the test data, together with any mathematical or statistical procedure used for data reduction and processing.

Appendix C: National Certification Test Design Criteria

Table of Contents

Appendix C: National Certification Test Design Criteria

C.1 Scope

This appendix describes the guiding principles used to design the voting system certification testing process conducted by the accredited test lab.

Certification tests are designed to demonstrate that the system meets or exceeds the requirements of the *Guidelines*. The tests are also used to demonstrate compliance with other levels of performance claimed by the manufacturer.

Certification tests must satisfy two separate and possibly conflicting sets of considerations. The first is the need to produce enough test data to provide confidence in the validity of the test and its apparent outcome. The second is the need to achieve a meaningful test at a reasonable cost, and cost varies with the difficulty of simulating expected real-world operating conditions and with test duration. It is the test designer's job to achieve an acceptable balance of these constraints.

The rationale for, and statistical methods of, the test designs required by the *Guidelines* are discussed below. Technical descriptions of these designs can be found in any of several books on testing and statistical analysis.

C.2 Approach to Test Design

The certification tests specified in the *Guidelines* are primarily concerned with assessing the magnitude of random errors. They are also, however, capable of detecting bias errors that would result in the rejection of the system.

Test data typically produce two results. The first is an estimate of the true value of some system attribute such as speed, error rate, etc. The second is the degree of certainty that the estimate is a correct one. The estimate of an attribute's value may or may not be greatly affected by the duration of the test. Test duration, however, is very important to the degree of certainty; as the length of the test increases, the level of uncertainty decreases. An efficient test design will produce enough data over a sufficient period of time to enable an estimate at the desired level of confidence.

There are several ways to design tests. One approach involves the pre-selection of some test parameter, such as the number of failures or other detectable factors. The essential element of this type of design is that the number of observations is independent of their results. The test may be designed to terminate after 1,000 hours or 10 days, or when 5 failures have been

observed. The number of failures is important because the confidence interval (uncertainty band) decreases rapidly as the number of failures increases. However, if the system is highly reliable or very accurate, the length of time required to produce a predetermined number of failures or errors using this method may be unachievably long.

Another approach is to determine that the actual value of some attribute need not be learned by testing, provided that the value can be shown to be better than some level. The test would not be designed to produce an estimate of the true value of the attribute but instead to show, for example, that reliability is at least 123 hours or the error rate is no greater than one in ten million characters.

The latter design approach, which was chosen for the *Guidelines*, uses what is called Sequential Analysis. Instead of the test duration being fixed, it varies depending on the outcome of a series of observations. The test is terminated as soon as a statistically valid decision can be reached that the factor being tested is at least as good as, or no worse than, the predetermined target value. A sequential analysis test design called the "Wald Probability Ratio Test" is used for reliability and accuracy testing.

C.3 Probability Ratio Sequential Test (PRST)

The design of a Probability Ratio Sequential Test (PRST) requires that four parameters be specified:

H0, the null hypothesis
H1, the alternate hypothesis
a, the producer's risk
b, the consumer's risk

The *Guidelines* anticipate using the PRST for testing both time-based and event-based failures.

This test design provides decision criteria for accepting or rejecting one of two test hypotheses: the null hypothesis, which is the Nominal Specification Value (NSV), or the alternate hypothesis, which is the MAV. The MAV could be either the Minimum Acceptable Value, or the Maximum Acceptable Value, depending upon what is being tested. Performance may be specified by means of a single value or by two values. When a single value is specified, it shall be interpreted as an upper or lower single-sided 90 percent confidence limit. If two values, these shall be interpreted as a two-sided 90 percent confidence interval, consisting of the NSV and MAV.

In the case of Mean Time Between Failure (MTBF), for example, the null hypothesis is that the true MTBF is at least as great as the desired value (NSV), while the alternate hypothesis is that the true value of the MTBF is less than some lower value (Minimum Acceptable Value). In the case of error rate, the null hypothesis is that the true error rate is less than some very small desired value (NSV), while the alternate hypothesis is that the true error rate is

greater than some larger value that is the upper limit for acceptable error (Maximum Acceptable Value).

C.4 Time-based Failure Testing Criteria

The equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision. Some of the performance test criteria of Volume II, Section 4, use this equivalence.

System acceptance or rejection can be determined by observing the number of relevant failures that occur during equipment operation. The probability ratio for this test is derived from the exponential probability distribution. This distribution implies a constant hazard rate for equipment failure that is not dependent on the time of testing or the previous failures. In that case, two or more systems may be tested simultaneously to accumulate the required number of test hours, and the validity of the data is not affected by the number of operating hours on a particular unit of equipment. However, for environmental operating hardware tests, no unit shall be subjected to less than two complete 24-hour test cycles in a test chamber as required by Volume II, Subsection 4.7.1.

In this case, the null hypothesis is that the Mean Time Between Failure (MTBF), as defined in Volume I, Subsection 4.3.3 is at least as great as some value, here the Nominal Specification Value. The alternate hypothesis is that the MTBF is no better than some value, here the Minimum Acceptable Value.

For example, a typical system operations scenario for environmental operating hardware tests will consist of approximately 45 hours of equipment operation. Broken down, this time allotment involves 30 hours of equipment setup and readiness testing and 15 hours of elections operations. If the Minimum Acceptable Value is defined as 45 hours, and a test discrimination ratio of 3 is used (in order to produce an acceptably short expected time of decision), then the Nominal Specification Value equals 135 hours.

With a value of decision risk equal to 10 percent, there is no more than a 10 percent chance that a system would be rejected when, in fact, with a true MTBF of at least 135 hours, the system would be acceptable. It also means that there is no more than a 10 percent chance that a system would be accepted with a true MTBF lower than 45 hours when it should have been rejected.

Therefore,

H0: MTBF = 135 hours
H1: MTBF = 45 hours
a = 0.10
b = 0.10.

Under this PRST design, the test is terminated and an ACCEPT decision is reached when the cumulative number of equipment hours in the second column of the following table has been reached, and the number of failures is equal to or less than the number shown in the first column. The test is terminated and a REJECT decision is reached when the number of failures occurs in less than the number of hours specified in the third column. Here, the minimum time to accept (on zero failures) is 169 hours. In the event that no decision has been reached by the times shown in the last table entries, the test is terminated, and the decision is declared as indicated. Any time that 7 or more failures occur, the test is terminated and the equipment rejected. If, after 466 hours of operation, the cumulative failure score is less than 7.0, then the equipment is accepted.

Number of Failures	Accept if Time Greater Than	Reject if Time Less Than
0	169	Continue test
1	243	Continue test
2	317	26
3	392	100
4	466	175
5	466	249
6	466	323
7	N/A	(1)

(1) Terminate and REJECT

This test is based on the table of test times of the truncated PRST design V-D in the Military Handbook MIL-HDBK-781A that is designated for discrimination ratio 3 and a nominal value of 0.10 for both a and b. The Handbook states that the true producer risk is 0.111 and the true consumer risk is 0.109. Using the theoretical formulas for either the untruncated or truncated tests will lead to different numbers.

The test design will change if given a different set of parameters. Some jurisdictions may find the Minimum Acceptable Value of 45 hours unacceptable for their needs. In addition, it may be appropriate to use a different discrimination ratio, or different, Consumer's and Producer's risk. Also, before using tests based on the MTBF, it should be determined whether time-based testing is appropriate rather than event-based or another form of testing. If MTBF-based procedures are chosen, then the appropriateness of the assumption of a constant hazard rate with exponential failures should in turn be assessed.

C.5 Accuracy Testing Criteria

Some voting system performance attributes are tested by inducing an event or series of events, and the relative or absolute time intervals between repetitions of the event has no significance. Although equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses event-based failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a device is usually dependent on the processing volume that it is required to perform. The elapsed time over which a certain number of actuation cycles occur is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data.

The error frequency, called “ballot position error rate,” applies to such functions as process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Certification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of ballot position error rate, the calculation for a specific device (and the processing function that relies on that device) is based on:

HO: Desired error rate = 1 in 10,000,000
H1: Maximum acceptable error rate = 1 in 500,000
a = 0.05
b = 0.05

and the minimum error-free sample size to accept for qualification tests is 1,549,703 votes.

The nature of the problem may be illustrated by the following example, using the criteria contained in the *Guidelines* for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is, the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:

a. The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million characters (including the null character)

b. If it can be shown that the system's true error rate does not exceed one in every five hundred thousand votes counted, it will be considered acceptable. This is more than accurate enough to declare the winner correctly in almost every election

c. A decision risk of 5 percent is chosen, to be 95 percent sure that the test data will not indicate that the system is bad when it is good or good when it is bad

This results in the following decision criteria:

d. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system

e. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted

f. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)